Meridian 1 and Succession Communication Server for Enterprise 1000

System Security Management

Document Number: 553-3001-302
Document Release: Standard 7.00
Date: January 2002

Copyright ©1993 – 2002 Nortel Networks
All Rights Reserved

Printed in Canada

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of the Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users will be required to correct the interference at their own expense.

SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Revision history

January 2002

Standard 7.00. This document is up-issued to include content changes for the Meridian 1 Release 25.40 and Succession Communication Server for Enterprise 1000 systems.

April 2000

Standard 6.00. This is a global document and is up-issued for Release 25.0x.

June 1999

Standard 5.00. This document is updated for Release 24.2x.

October 1997

Standard 4.00. This document is updated for Release 23.0x.

July 1995

Standard 3.00. This document is issued to include Release 21 changes.

December 1994

Standard 2.00. Includes Release 20 changes, editorial changes, and indexing.

October 31, 1993

Standard 1.00.

Contents

About this document 9
Purpose of this document 9
Who should read this document 10
What is in this document 10
Related documents 11

Introduction 13
System security overview 13
General security practices 15

System security features 17
Contents 17
Introduction 19
Defining basic access restrictions 19
Modifying basic access restrictions 25
System Access Enhancements 49
Using system management features 53
Controlling Call Forward access 56
Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS) 61
Controlling Direct Inward System Access 69
Controlling Multi-Tenant Services 71

Meridian Mail security features 75
Contents 75
Reference list 76
Introduction 76
Controlling mailbox features 76
Controlling Voice Menu/Thru-dialer 79
Fax on Demand 79
Controlling mailbox access 79
Controlling the administration terminal 82
Controlling Outcalling 83
Controlling the Meridian Mail virtual agents 84
Controlling upgrades 84
Controlling AMIS networking 85

System access security features 87
Contents 87
Controlling access to administration programs 87
Recommended password management practices 89
Controlling access to the system 95
Controlling access to system Application Processors 103

New system security planning 107
Contents 107
Introduction 108
Analyzing the system configuration 109
Filling out the security installation checklist 109
System checklist 110
Basic Access Restrictions 110
Modifying Basic Access Restrictions 111
Traffic Reporting (TFC) 123
Meridian Mail checklist 123

Existing system security upgrade 127
Contents 127
Introduction 128
Auditing system security features 129
System audit checklist 129
Auditing Meridian Mail security features 157
Meridian Mail audit checklist 157
Auditing Application Processor security features 163

System security features verification 165
Contents 165
Introduction 166
Verify system security features using the checklist 166
Verify Call Forward access restrictions 167
Verify DISA access restrictions 168
Verify BARS/NARS access restrictions 169
Verify administration program access restrictions 171
Verify Thru-dial restrictions for mailboxes and menus 172

System security analysis 175
Contents 175
Reference list 175
Introduction 176
Using the system reports summary 176
Analyzing Call Detail Recording reports 178
Analyzing Traffic Measurement reports 182
Checking the History File 195
Analyzing Operational Measurement reports 196

Appendix A: Access Restriction features 201

Appendix B: Trunk Group Access Restrictions worksheet 205

Index 211

About this document

This document applies to the Meridian 1 Internet Enabled and the Succession Communication Server for Enterprise (CSE) 1000 systems.

This document is a global document. Contact your system supplier or your Nortel Networks representative to verify that the hardware and software described is supported in your area.

Purpose of this document

The purpose of this document is to instruct system distributors and administrators on how to detect possible unauthorized access to the system and Meridian Mail, and how to implement system-wide security features. This document describes how to:

- plan and implement security options for a new system
- audit an existing system's security
- upgrade an existing system's security features where necessary

This document also describes how to verify that security features are in place and how to use built-in system monitoring and reporting facilities to discover fraudulent and unauthorized use of telecommunications facilities.

This document addresses the security issues that are PBX-specific such as toll fraud, unauthorized use of features, and unauthorized access to the system. It does not address non-system specific security issues. It is assumed that LAN/WAN administrators have implemented their own network security policies.

Who should read this document

This document is intended to help distributors and system administrators who are installing new systems and upgrading and maintaining existing systems. It is assumed that the reader has a thorough knowledge of system software and Meridian Mail software operations and has the ability to configure and maintain systems using configuration and maintenance programs.

What is in this document

This document contains the following chapters:

- **Introduction** is an overview of how to prevent unauthorized access and provide security practices for the system.
- **System security features** describes these features and explains how to implement security for system call processing by limiting and controlling call privileges and restricting access to system facilities and features.
- **Meridian Mail security features** describes these features and explains how to implement security for Meridian Mail by limiting and controlling access to Meridian Mail features and mailboxes.
- **System access security features** describes these features and explains how to implement security features to control access to system administration and maintenance functions, Meridian Mail administration terminals, and Application Processors.
- **New system security planning** describes how to plan new system security based on the customer configuration database generated for the system and the facilities and features available on the system.
- **Existing system security upgrade** explains how to plan an existing system security upgrade by auditing the configuration and defining additional security features as required.
- **System security feature verification** describes how to verify that all system security features have been correctly implemented by following the provided checklist and testing procedures to verify the features that were implemented.
- **System security analysis** explains how to use call detail recording, traffic measurement, history file, and audit trail information to monitor system administration activities and traffic patterns.

Related documents

Refer to the following documents for additional information:

- *System Management* (553-3001-300)
- *System Management Applications* (553-3001-301)
- *Software Input/Output Guide Administration* (553-3001-311)
- *Features and Services* (553-3001-306)
- *Meridian Mail General Description* (553-7001-100)
- *Meridian Mail System Administration Guide* (553-7001-302)
- *Meridian Mail System Administration Tools* (553-7001-305)
- *Meridian Mail Maintenance Messages* (553-7001-510)

Introduction

This chapter is an overview of how to control unauthorized access and provide security for the system. It describes the reason for implementing system security and provides recommendations for preventing abuse and damage to the telecommunications facilities.

System security overview

Each telecommunications system must be protected from unauthorized and fraudulent use. The system can be vulnerable to abuse by employees as well as outside sources. Security requirements for each system are unique and are based on the system configuration, functions, and features it supports.

Access to these functions and features must be controlled by safeguards implemented in the system. Exercise caution when handling and disposing of information that can compromise system security. Inadequate control of calling privileges and unprotected physical access to switching systems are the main reasons companies incur fraudulent expenses through use of their telecommunications facilities.

One of the most serious sources of toll fraud is unauthorized remote access to a second dial tone through the system. This feature is called Direct Inward System Access (DISA). DISA privileges are intended for traveling employees who call into their company's PBX, enter an access code, and then use the company's long distance calling services instead of using a credit card or letting the operator handle the call. Telecommunications managers must strictly monitor and control access privileges.

Voice mail and automated attendant services are also major targets. Without proper safeguards, callers accessing a voice mail system can easily place toll calls once they know long distance access codes or trunk access codes. They can also take over a mailbox for use as a bulletin board.

Remote system administration can be vulnerable to unauthorized access. Remote system administration allows PBX technicians to access, configure, and troubleshoot both the system and Meridian Mail software and hardware problems remotely. Without properly safeguarding maintenance ports, an unauthorized person can access the system, change the system configuration, degrade system performance, and fraudulently use PBX services.

An intruder can dial into a remote access port and, once the password is determined, access the system, change the customer database configuration to allow international calls, enable the DISA feature, turn off Call Detail Recording, and defeat any safeguards already in place.

By activating traffic and call detail reports, checking calling patterns, and looking for variations, PBX fraud, which occurs mostly at night, on weekends, and on holidays, can usually be detected.

Typical patterns for outgoing call fraud are:

- calls to unusual locations,
- high call volume,
- long call duration,
- international calls, and
- unexplained 900 number calls.

The primary call destinations for toll fraud are international and the 809 area code.

Incoming call patterns that must be investigated are long holding times, an unexplained surge in traffic, and higher than usual traffic after business hours. If no traffic is being reported when some traffic is expected, this can indicate that the CDR reporting was deactivated and a maintenance port has been compromised.

Secure the system by knowing the current system software configuration, knowing which security features are active, and monitoring calling patterns to detect unauthorized activity.

General security practices

Each telecommunications facility must be protected by a security program to prevent unauthorized and fraudulent use. Failure to implement a security program when the PBX is first installed, neglecting to carefully monitor system traffic patterns and system messages, and neglecting to improve system security as additional services are added, will make the system vulnerable.

In addition, practice the following system security recommendations to minimize the possibility of fraud:

- Deny unauthorized access to long distance trunk facilities (thru-dial) when using voice mail. This can be accomplished by requiring a password to access the feature or by blocking its activation.
- Require outside callers to use authorization codes when making incoming calls to DISA lines. Never publish DISA numbers. For greater security, use maximum length authorization codes that do not include an employee identification number, home telephone number, or social security number as part of the authorization code.
- Safeguard system configuration printouts, call detail records, and authorization code printouts. Dispose of this information in the same way as any other confidential information.
- Change all authorization codes as often as is practical. A maximum interval of 60 days is recommended. Delete codes used by former employees. Treat authorization codes like credit card numbers. Do not allow employees to share authorization codes.
- Restrict DISA calls at night and on holidays, if possible. Unauthorized calls are usually placed during these times.
- Monitor traffic patterns and call detail records to detect unusual traffic patterns and unauthorized calls.
- Provide international calling privileges only to users who require them. Restrict international calls only to countries that authorized users normally call; otherwise, block international calls completely.
- Restrict call forwarding so that telephones cannot forward calls to long distance numbers or trunk facilities.

- Do not allow employees to post access codes, authorization codes, and passwords in plain view.
- Restrict switchroom access to authorized personnel.
- Implement a system security policy that includes the following:
  - password management
  - program access control
  - Problems Determination Tool (PDT) access control
  - administration port security
  - Audit Trail review
  - History File review

Follow these recommendations, analyze the existing security plan regularly, and upgrade that plan when required to minimize the opportunity for unauthorized persons to abuse and damage the telecommunications facilities.

The following chapters describe system security planning, and implementing and verifying procedures to provide better telecommunications system security.

System security features

Contents

This section contains information on the following topics:

Defining basic access restrictions. 19
- Class of Service. 20
- Trunk Group Access Restrictions. 23

Modifying basic access restrictions. 25
- System Speed Call. 26
- Network Speed Call. 27
- Authorization Code. 28
- Forced Charge Account. 32
- Controlled Class of Service. 32
- Enhanced Controlled Class of Service 33
- Electronic Lock. 34
- Code Restriction Data Block. 35
- New Flexible Code Restriction. 36
- Called Party Disconnect Control. 36
- Scheduled Access Restrictions. 37
- Trunk Barring. 46

System Access Enhancements. 49
- Default Class of Service (CLS). 50
- Default Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG) 51
- Call Forward Default Length and Range. 52
- Security Banner at System Login. 52
- Failed Login Attempt Threshold 52
- PWD2/PWD1/LAPW Passwords and LAPW Login names 53

Problems Determination Tool (PDT) Access Information. 53
Using system management features. 53
Electronic Switched Network (ESN) Database. 53
Trunk and Route Database. 54
System Management Base. 55
Controlling Call Forward access. 56
User Selectable Call Redirection. 57
Call Forward External Deny. 57
Internal Call Forward. 58
Call Forward All Calls 59
Call Forward to Trunk Access Code. 59
Call Forward Originating or Forwarded Class of Service. 60
Remote Call Forward. 61
Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS). 61
Supplemental Digit Recognition/Restriction. 62
Network Class of Service and Facility Restriction Level. 63
Authorization Code Conditionally Last Network Authorization Codes 64
Time-of-Day Routing. 65
Routing Control. 66
Incoming Trunk Group Exclusion. 67
Free Calling Area Screening. 68
Controlling Direct Inward System Access. 69
Security Code. 70
Authorization Code. 71
Service restrictions. 71
Controlling Multi-Tenant Services. 71
Tenant-to-Tenant Access. 72
Tenant-to-Route Access. 72
Console Presentation Group (CPG) assignment. 73

Introduction

This chapter describes the system call processing security features and how to implement them. This is done by limiting and controlling call privileges and restricting access to the system facilities and features. Call processing privileges and restrictions are implemented by the following:

- Defining basic access restrictions
- Modifying basic access restrictions
- System Access Enhancements
- Using system management features
- Controlling Call Forward access
- Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)
- Controlling Direct Inward System Access
- Controlling Multi-Tenant Services

Defining basic access restrictions

Basic access restrictions allow internal and external users to be assigned access to only the facilities and calling privileges their jobs require. In this way, internal abuse can be deterred and external access to toll facilities can be restricted. The following features control access restrictions:

- Class of Service (CLS)
- Trunk Group Access Restrictions (TGAR)

CLS and TGAR work together to control specific trunk groups to which telephones, DISA directory numbers, TIE trunks, and Authcodes have direct access. They determine whether users can make local, TIE, or long distance calls over these trunks.

Class of Service

Class of Service (CLS) provides the flexibility to group telephones, DISA directory numbers, TIE trunks, and Authcodes. CLS assigns to these groups the calling privilege Levels that suit the groups' communications needs. CLS can help protect the system from internal abuse by preventing internal users from placing unauthorized toll calls.

Assign any one of the following Classes of Service to each telephone, DISA directory number, TIE trunk, and Authcode to control the degree of access to the exchange network:

- **Unrestricted Service (UNR) –** Allowed to originate and receive calls to and from the exchange network.
- **Conditionally Unrestricted (CUN) –** Allowed to receive calls from the exchange network. Toll-denied for calls placed using direct access to trunks, but unrestricted for toll calls placed through Automatic Number Identification (ANI).
- **Conditionally Toll-Denied (CTD) –** Allowed to receive calls from the exchange network. Toll-denied for calls placed using direct access to the Central Office (CO), Foreign Exchange (FEX), and two-way Direct Inward Dial (DID) trunks, but unrestricted for toll calls placed through BARS/NARS using Network Class of Service (NCOS). CTD is most effective when used in conjunction with Trunk Group Access Restrictions (TGAR).
- **Toll-Denied Service (TLD) –** Allowed to receive calls from the exchange network and to dial local exchanges. Calling privileges of toll-denied telephones can be modified using Code Restriction (CRB) or New Flexible Code Restriction (NFCR) or Forced Charge Account (FCA) to allow or deny certain dialing sequences using direct trunk access.
- **Semi-Restricted Service (SRE) –** Allowed to receive calls from the exchange network. Restricted from dial access to the exchange network but allowed access to TIE trunks. Allowed to access the exchange network through an attendant or an unrestricted telephone.
- **Fully Restricted Service –** The following classes of Fully Restricted Service are available:

— **FRE –** Allowed to originate and receive internal calls. Allowed access to TIE and CCSA networks, and to and from the exchange network using call modification from an unrestricted telephone. Denied access, either through dialing or through the attendant, to and from the exchange network.

— **FR1 –** Allowed to originate and receive internal calls. Allowed access to TIE and Controlled Class of Service Allowed (CCSA) networks. Denied access to and from the exchange network.

— **FR2 –** Allowed to originate and receive internal calls. Denied access to TIE and CCSA networks and to the exchange network.

Table 1 on page 21 outlines various call types and shows whether they are possible for each CLS assignment.

Table 1
CLS assignment (Part 1 of 2)

	UNR	CTD/ CUN	TLD	SRE	FRE	FR1	FR2
Incoming trunk calls	Yes	Yes	Yes	Yes	Yes using call modification	No	No
Outgoing non-toll trunk call	Yes	Yes	Yes	Yes using attendant or UNR telephone	Yes using UNR telephone	No	No
Outgoing toll trunk call (0 or 1+ on COT or FX)	Yes	Yes using BARS/ NARS No direct access	Yes using attendant or UNR telephone No direct access	Yes using attendant or UNR telephone No direct access	Yes using UNR telephone No direct access	No	No

Table 1
CLS assignment (Part 2 of 2)

	UNR	CTD/ CUN	TLD	SRE	FRE	FR1	FR2
To/from TIE trunk	Yes	Yes	Yes	Yes	Yes	Yes	Yes
To/from internal	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BARS/ NARS calls TGAR=No	Uses NCOS only	Uses NCOS only	Uses NCOS and CLS	Uses NCOS and CLS	Uses NCOS and CLS	Uses NCOS and CLS	Uses NCOS and CLS
BARS/ NARS calls TGAR=Yes	Uses NCOS and TGAR	Uses NCOS and TGAR	Uses NCOS, CLS, and TGAR	Uses NCOS, CLS, and TGAR	Uses NCOS, CLS, and TGAR	Uses NCOS,CLS, and TGAR	Uses CLS only

Table 2 lists the facilities that can be implemented using CLS, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 2
Implementing CLS

Facility	Overlay and prompts	Print programs
Telephones	LD 10/11 – CLS	LD 10/11 by TN LD 81 by CLS
Authcodes	LD 88 – CLS	LD 88 by Authcode
DISA	LD 24 – TGAR	LD 24 by DN

Trunk Group Access Restrictions

Trunk Group Access Restrictions (TGAR) control access to trunks that interface with the exchange network, TIE and CCSA networks, and services such as paging, dictation, and recorded announcements.

Telephones, DISA directory numbers, TIE trunks, and Authcodes are assigned to TGAR groups. When users attempt to access trunk routes from telephones, TIE trunks, or Authcodes, the system uses their TGAR assignment to check whether they can access that trunk. All trunks are assigned to a Trunk Access Restriction Group (TARG). If the TGAR assignment of the telephone, DISA directory number, TIE trunk, or Authcode is the same as the TARG assigned to the trunk, direct access is blocked. If TARG and TGAR do not match, or either assignment is set to 0, then access is allowed. If access is permitted, the system uses the CLS assignment to determine call eligibility. The system always uses the most restrictive assignment (CLS or TGAR) to determine call eligibility when users try to directly access trunk facilities.

Limiting trunk access prevents users from generating unnecessary toll charges. It also limits long distance calling capabilities of virtual voice mail agents and data ports.

> ***Note:*** The BARS/NARS least cost routing software eliminates the need for direct access to outbound facilities for long distance calls. TGARs can be used in conjunction with BARS/NARS, if required. Refer to "Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)" on page 61.

Table 3 lists the facilities that can be implemented using TGAR, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 3
Implementing TGAR

Facility	Configuration program and prompt	Print program
Telephones	LD 10/11 – TGAR	LD 10/11 by TN
Authcodes	LD 88 – TGAR	LD 88 by Authcode
TIE Trunks	LD 14 – TGAR	LD 20 by TN
Trunk Groups (Route)	LD 16 – TARG	LD 21 by route, access code
DISA	LD 24 – TGAR	LD 24 by DN

Table 4
TGAR Routing

Route #	Rank type
Route 0	COT
1	WATS
2	FX 1
3	FX 2
4	TIE 1
5	TIE 2
6	Paging

In the example shown in Table 5, assume the following seven TGAR codes are required:

Table 5
TGAR Access Restriction Codes

TGAR	Access denied to routes
0	No restrictions
1	0,1,2,3,4,5,6 (default = 1)
2	2,3,4,5
3	3,4,5
4	2,6
5	3,4,5,6
6	5,6

Modifying basic access restrictions

Occasionally, the basic access restrictions that have been implemented may have to be changed. The following features can be used to selectively override CLS and TGAR when it is necessary to extend a DISA directory number's, telephone's, or TIE trunk's normal calling capabilities:

- Outgoing Call Barring
- System Speed Call
- Network Speed Call
- Authorization Code
- Forced Charge Account
- Controlled Class of Service
- Enhanced Controlled Class of Service
- Electronic Lock

- Code Restriction
- New Flexible Code Restriction
- Called Party Disconnect Control
- Scheduled Access Restrictions
- System Access Enhancements

System Speed Call

System Speed Call (SSC) extends the capabilities of Speed Call. In addition to providing abbreviated dialing, using entries in SSC lists lets internal users temporarily override the NCOS assigned to telephones and place calls to telephone numbers in the SSC list. With this feature, the most appropriate NCOS can be assigned to a telephone to limit the potential for unauthorized calling, and at the same time allow calls to approved destinations.

Telephones can be assigned to different SSC lists. These telephones can also be designated as either System Speed Call Users (SSUs) or as System Speed Call Users/Controllers (SSCs) on the list. A user/controller can use the list to add or delete telephone numbers from it. Controller capabilities must be assigned only as the job function dictates, in order to minimize abuse. Usually, only one controller is assigned to each SSC list.

List controlling capabilities can be assigned to a key on the attendant console. However, this key does not override CLS and TGAR because the attendant is not subject to these restrictions.

> ***Note:*** An SSC list can also override the telephone restrictions imposed through BARS/NARS. See “Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)” on page 61.

Table 6 on page 27 lists the facilities that can be implemented using SSC, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 6
Implementing SSC

Facility	Overlay and prompts	Print programs
Telephones	LD 10 - FTR	LD 10 by TN
	LD 11- SSU, KEY	LD 81 by SSU, SSC, KEY, LD 11 by TN
Flexible Feature Code	LD 57 - SSPU	LD 57 by FFC Data
Speed Call List	LD 18 - SSC, all prompts	LD 20 by List Number
Attendant	LD 12 - KEY	LD 20 by TN

Network Speed Call

Network Speed Call (NSC) expands the SSC capabilities by allowing users to access the NSC feature from public and private networks. This enables users who are normally restricted from making certain types of BARS/NARS calls to make these calls if the destination is a company-approved number defined in an NSC list.

Use this feature in conjunction with a restricted DISA directory number. The incoming DISA caller can gain access to approved destinations using the NSC list. This feature helps prevent abuse by allowing calls to be placed only to destinations on NSC lists.

Table 7 on page 28 lists facilities that can be implemented using NSC, programs and prompts to implement the feature, and programs to print information about the feature.

Table 7
Implementing NSC

Facility	Overlay and prompts	Print programs
Network translation	LD 90 -TYPE = NSCL all prompts	LD 90 by NSC Access Code
SSC	LD 18 - TYPE = SSC all prompts	LD 20 by SSC list
Network Control	LD 87 FEAT = NCTL NSC, LIST	LD 87 by NCTL
Authcode	LD 88 TYPE = AUT, CODE, CLAS	LD 88 by Authcode
Telephones	LD 10 and LD 11 - NCOS	LD 10/11 by TN LD 81 by NCOS
Trunk	LD 14 - NCOS	LD 20 by TN
Customer	LD 15 - NCOS, FCNC, NET	LD 21 by NET
SSC list	LD 18 - NCOS	LD 20 by Speed Call List
DISA	LD 24 - NCOS	LD 24 by DISA directory number

Authorization Code

Authorization Codes (Authcodes) enable users to temporarily override access restrictions assigned to telephones, DISA directory numbers, or TIE trunks. A user enters an Authcode that has an associated CLS, TGAR, and BARS/NARS NCOS. The user has the calling privileges of the Authcode rather than those of the DISA directory number, telephone, or TIE trunk for the duration of the call.

This allows users to place calls from normally restricted telephones. These restricted telephones can be located in areas of public access where authorization codes are required or can be used without authorization codes by employees who do not require broader calling privileges.

The system offers Station Specific Authcodes, which allows the administrator to define the authorization code access Level for each telephone. To verify the validity of the code, the system checks Overlays 10, 11, and 88. To delete an Authcode, the administrator must delete it from Overlays 10, 11, and 88.

There are three Levels of Authcode access:

1 **Authcode Unrestricted (AUTU) –** allows a telephone set to enter any authorization code without additional restrictions.

2 **Authcode Restricted (AUTR) –** requires that the entered authorization code must match one of the preassigned authorization codes. Any other Authcode will be treated as invalid and an error message will be generated at the TTY.

3 **Authcode Denied (AUTD) –** does not accept Authcode entries from a telephone set as AUTD.

Authcode Alarm

The system offers an Authorization Code Security feature enhancement that enables a user to temporarily override access restrictions assigned to a station or trunk because of their assigned Network Class of Service (NCOS), Class of Service (COS), and Trunk Group Access Restrictions (TGAR) codes. If a user requires access to system facilities in addition to those allowed on the telephone, the Authcode feature can be used to provide them.

In addition, the Authorization Code (Authcode) Alarm feature alerts the technician when an invalid Authcode is entered, by generating an Authcode Alarm. The alarm indicates to the technician that an unauthorized person may be trying to use an Authcode to illegally access the switch.

The Authcode alarm is generated upon detection of violation of all Authcode-related features (such as Basic, Network, Station Specific Authorization code features, and Security Administration (SECA), except for calls originated by the attendant. The SECA alarm distinguishes security violation from other types of system messages. These messages will be printed on the TTY.

The Authcode Alarm feature does not apply to calls originated by an attendant.

The Authcode alarm feature is enabled through the Authcode Data Block LD 88.

LD 88 – Enable the Authcode alarm feature.

Prompt	Response	Description
REQ	NEW CHG	Add. Change.
TYPE	AUB	Authcode Data Block.
CUST	xx	Customer number.
SPWD	xxx	Secure data password.
ALEN	1-14	Number of digits in Authcode.
ACDR	(NO) YES	(Do not) activate CDR for authcodes.
AUTHCOD_ALRM	(OFF) ON	(Disable) enable Authcode Alarm.

LD 17 – Configure the Alarm Filter table as per existing configuration procedures. The Authcode Alarm must be configured in this table in order for the messages to be displayed on the FIL TTY.

Authcodes can be recorded as part of Call Detail Records so that call patterns can be observed, and calls billed back to the appropriate department or person.

Note: Authcodes can be used to override telephone restrictions imposed through BARS/NARS. See "Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)" on page 61.

Table 8 lists the facilities that can be implemented using the Authcode feature, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 8
Implementing Authcode

Facility	Overlay and prompts	Print programs
Authcodes	LD 88 – all prompts	LD 88 by Authcode
Secure Data Password	LD 15 – SPWD, PWD2 and LD 88 – SPWD	LD 22 Passwords
Authcodes by telephone	LD 10/11 – CLS: (AUTU), AUTR, AUTD MAUT: YES/NO SPWD: (if MAUT=YES) AUTH: x nnnn	LD 10/11 by TNB
Authcodes by feature	LD 81 – FEAT: AUTU, AUTR, AUTD	LD 81 by FEAT
Authcode Alarm*	LD88 – AUTHCOD_ALRM and LD17 – AUTHCOD_ALRM	
*For security reasons, the SECA00001 alarm must not be configured in the Exception Filter table.		

Forced Charge Account

Forced Charge Account (FCA) temporarily overrides toll-denied CLS restrictions when users enter account codes before placing toll calls. Account codes allow users to have a customer-defined FCA Network Class of Service for the duration of calls.

Call Detail Recording outputs a charge record that identifies the charge account used for the call.

> ***Note:*** FCA can also be used to override restrictions imposed through BARS/NARS. See "Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)" on page 61.

Table 9 lists the facilities that can be implemented using FCA, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 9
Implementing FCA

Facility	Overlay and prompts	Print programs
Customer	LD 15 - CHLN, FCAF, CHMN, FCNC, CDR	LD 21 by CDR
Telephones	LD 10/11 - CLS = TLD, FCAR	LD 10/11 by TN
TIE Trunks	LD 14 - CLS = TLD, FCAR	LD 20 by TN

Controlled Class of Service

Controlled Class of Service (CCOS) allows the following users to temporarily alter telephone CLS:

- users of digital telephones designated as controllers
- users of TTYs designated as Background Terminals

When a telephone is in the controlled mode, its CLS is derived from the CLS restriction Level defined for each customer. This prevents internal abuse by reducing the CLS for telephones in vacant areas.

Users of digital telephones designated as controllers can place telephones in a controlled mode one at a time and Background Terminals can alter individual, group, or all designated telephones at one time.

Table 10 lists the facilities that can be implemented using the CCOS feature, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 10
Implementing CCOS

Facility	Overlay and prompts	Print programs
Customer	LD 15 - CCRS, CCOS	LD 21 by CCOS
Telephones to be controlled	LD 10/11 - CLS	LD 20 by TN
Telephones to be controllers	LD 11 - KEY	LD 20 by TN
Background Terminal	LD 17 - ADAN, USER	LD 22 by ADAN

Enhanced Controlled Class of Service

Enhanced Controlled Class of Service (ECCS) extends the controller function of CCOS to attendant consoles and M3000 terminals equipped with a Controller Key. It also allows for two additional customer-defined Levels of CCOS restrictions. This helps to further control calling privileges of telephones in unsecured areas and helps prevent unauthorized access to toll calls.

Table 11 on page 34 lists the facilities that can be implemented using the ECCS feature, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 11
Implementing ECCS

Facility	Overlay and prompts	Print programs
Customer	LD 15 – CCRS, ECC1, ECC2, CCOS	LD 21 by Data group
Telephones to be controlled	LD 10/11 – CLS	LD 10/11 by TN
Telephones to be controllers	LD 11 – KEY	LD 11 by TN
Attendants to be controllers	LD 12 - KEY	LD 20 by TN
Background Terminal	LD 17 - USER	LD 22 by Data group

Electronic Lock

Electronic Lock (ELK) allows users to activate and deactivate CCOS mode from their telephones by entering the Station Control Password (SCPW) and the appropriate ELK code.

Define the Station Control Password Length (SCPL) for each customer. If SCPL is set to 0, ELK and RCFW are disabled. Use a unique four to six digit password for each telephone.

Telephone users can activate ELK to prevent unauthorized calls from their telephones when they are not able to restrict physical access to these telephones. This is particularly useful for evenings, weekends, vacations, and holidays.

Table 12 lists the facilities that can be implemented using ELK, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 12
Implementing ELK

Facility	Overlay and prompts	Print programs
Customer	LD 15 - CCRS, SCPL, CCOS	LD 21 by Data group
Flexible Feature Code	LD 57 - FFCT, CODE, ELKA, ELKD	LD 57
Telephones	LD 10/11 - SCPW, CLS	LD 10/11 by TN

Code Restriction Data Block

Code Restoration Data Block (CRB) gives toll-denied telephones and TIE trunks limited access to the toll exchange network over CO and FEX trunks. For each CO and FEX trunk group, build a CRB that specifies the allowed area codes and/or exchange codes for toll-denied users accessing those facilities. This feature limits access to approved toll exchange networks and also limits the unauthorized use of toll facilities.

Table 13 lists the facilities that can be implemented using CRB, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 13
Implementing CRB

Facility	Overlay and prompts	Print programs
CRB	LD 19 all prompts	LD 21 by Route
Telephones	LD 10/11 - CLS = TLD	LD 81 by TLD LD 10/11 by TN

New Flexible Code Restriction

New Flexible Code Restriction (NFCR) enhances CRB by allowing toll-denied telephones, TIE trunks, and Authcodes to selectively make certain calls on outgoing trunk routes.

Assign toll-denied users a Network Class of Service (NCOS), and allow or deny calling privileges according to the Facility Restriction Level (FRL) of the NCOS.

Table 14 lists the facilities that can be implemented using NFCR, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 14
Implementing NFCR

Facility	Overlay and prompts	Print programs
Customer	LD 15 - NFCR, MAXT	LD 21 by NFCR
Network Control	LD 87 - NCOS, FRL	LD 87 by NCOS
NFCR Block	LD 49 - FCR all prompts	LD 49 by Table
Route	LD 16 - FRL	LD 21 by Route
Telephone	LD 10/11 - NCOS CLS=TLD	LD 10/11 by TN LD 81 by TLD, NCOS

Called Party Disconnect Control

Called Party Disconnect Control (CPDC) controls the disconnection of calls on CO, FEX, CCSA, DID, TIE, WATS, modem, and Central Automatic Message Accounting (CAMA) trunks.

Incoming trunk calls answered within the system are not disconnected until the called party hangs up. If the calling party hangs up, the connection is held allowing the call to be traced in emergency situations. If the calling party lifts the receiver again, the call is not reestablished.

CPDC prevents trunk-to-trunk transfers. A route assigned CPDC cannot be transferred to another route for outbound traffic.

Table 15 lists the facilities that can be implemented using CPDC, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 15
Implementing CPDC

Facility	Overlay and prompts	Print programs
Trunk Group (Route)	LD 16 - CPDC	LD 21 by ROUT or ACOD

Scheduled Access Restrictions

The Scheduled Access Restrictions (SAR) feature allows a customer to define Trunk Group Access Restrictions (TGAR), Class of Service (COS) restrictions, and Network Class of Service (NCOS) restrictions for different hours and days (typically off-hours and off-days).

These TGAR, COS, and NCOS restrictions comprise SAR groups. Each customer can define up to 1000 SAR groups, and one of these groups can be assigned to each customer station or route. Up to eight time periods can be defined for each SAR group, and different restrictions can be applied to each time period.

SAR can be overridden on a single call basis for a station or route by using an authorization code or forced charge account. By using the Scheduled Access Restrictions Disable (SARD), Scheduled Access Restrictions Enable (SARE), Scheduled Access Restrictions Lock (SARL), or Scheduled Access Restrictions Unlock (SARU) Flexible Feature Codes (FFC), these restrictions can be changed on a more permanent basis.

SARD returns the telephone/route to its normal restriction state. SARE cancels SARD, returning the telephone to its SAR state. SARL occurs automatically at a predefined period of time or when the Lock command is dialed by the user. Lock restrictions remain in effect until an SARU or SARD command is entered. The SARL command can be used on a customer basis or SAR group basis, depending on the Authcode used.

The Flexible Feature Codes can be used to do the following:

- extend off-hour restrictions for weekends or holidays (SARL)
- return to the schedule of access restrictions (SARU)
- extend normal restrictions into the off-hour period for after hour services (SARD)
- cancel after hour services (SARE)
- cause off-hour restrictions to start immediately (SARL followed by SARE)
- disallow any calls on an Attendant Console (SARL or SAR group containing the attendant(s)).

Customer attendants that are included in SAR groups are placed in Position Busy when an off-hour or off-day period goes into effect. The restricted attendant can only release existing calls or dial the SAR Flexible Feature Codes. New calls cannot be made. Incoming calls are directed to any other attendants that are not included in SAR groups and that are not in Position Busy.

If the system is placed in Night Service by an attendant, or the system is automatically placed in Night Service because all attendants are in the Position Busy state, incoming calls are routed to the Night DN. Going into Night Service automatically places attendants who belong to a SAR group into SAR Locked and Enabled state. These attendants can only release existing calls or dial the SAR Flexible Feature codes; they cannot make new calls when restricted by SAR.

Operating parameters

The definition of authorization codes for SAR decreases the number of authorization codes available for non-SAR use.

SAR does not apply to Direct Inward System Access (DISA) DNs. DISA can be used to manually modify the SAR schedule using an FFC authorization code.

Telephones and trunks assigned to SAR groups have their Class of Service (COS), Trunk Group Access Restriction (TGAR), and Network Class of Service (NCOS) defined by the SAR schedule of their SAR group.

During the periods that a SAR or SAR lock is in effect, the Controlled Class of Service (CCOS) for the station or trunk is overridden.

If a Facility Restriction Level (FRL) is changed in order to be associated with a different New Flexible Code Restriction (NFCR) tree, the NCOS using that FRL is affected. Also, different FRLs and, therefore, different NFCR trees are used at different times according to the NCOS assigned to the SAR group.

Feature interactions

- Basic Automatic Route Selection

  If SAR is equipped when Basic Automatic Route Selection (BARS) is set up, an NCOS value between 0 and 99 must be defined for each time period.

- Coordinated Dialing Plan

  If SAR is equipped when Coordinated Dialing Plan (CDP) is set up, an NCOS value between 0 and 99 must be defined for each time period.

- Call Detail Recording

  If configured, Call Detail Recording (CDR) A-type records are printed for SAR Flexible Feature Code functions.

- Network Alternate Route Selection

  If SAR is equipped when Network Alternate Route Selection (NARS) is set up, an NCOS value between 0 and 99 must be defined for each time period.

- Speed Call and Network Speed Call

  The System Speed Call and Network Speed Call features ignore the Class of Service and TGAR access restrictions in a SAR schedule, using the Class of Service and NCOS defined in the Speed Call List.

- Office Data Administration System

  Office Data Administration system (ODAS) can be used to indicate that telephones have been assigned to a SAR group. ODAS must be equipped in order to print members of a SAR group in LD 81.

- Controlled Class of Service (CCOS)

  If SAR is active, it overrides CCOS whether activated by a controller or Electronic Lock.

- Multi-Tenant Service

  If a SAR is assigned to a tenant, any telephone belonging to the tenant will follow this SAR schedule unless the telephone belongs to a SAR group. The telephone's Scheduled Access Restrictions override any SAR assigned to the tenant.

Feature packaging

This feature requires Scheduled Access Restrictions (SAR) package 162. SAR package 162 also requires the following:

- Flexible Feature Codes (FFC) package 139 and Basic Authorization Code (BAUT) package 25 add capability for manual modification of the schedules.
- Call Detail Recording (CDR) package 4, must be equipped if CDR is required.
- Network Class of Service (NCOS) package 32 must be equipped to make Network Class of Service (NCOS) restrictions effective.
- Charge Account for CDR (CHG) package 23, Charge Account/Authorization Code Base (CAB) package 24, and Forced Charge Account (FCA) package 52, can be equipped for additional billing information.
- The following packages are also required:

— Network Authorization Code (NAUT) package 63

— Multi-Tenant Service (TENS) package 86

Feature implementation

LD 88 – Create or modify Schedule Access Restrictions.

Prompt	Response	Description
REQ	NEW CHG	Add, or change.
TYPE	SAR	Scheduled Access Restrictions.
CUST	xx	Customer number.
SPWD	xxxx	Secure data password (same password as defined for DISA on a per customer basis in LD 15). **Note:** The SPWD prompt does not appear to a user with an LAO password.
SGRP	0-999	SAR group number.
SCDR	(NO) YES	(Do not) activate CDR for the SAR FFC commands.
OFFP	1-8	Off-hour period number. Off-hour periods can overlap; the period that starts first has priority until that off-hour period is over.
	<cr>	Go to ICR prompt.
- STAR hh mm	hh mm	Start time. The current start time (hours and minutes) is printed individually after the prompt. Respond with the new start time.
	X	Remove value and return to OFFP prompt.
-STOP hh mm	hh mm	Stop time.

Prompt	Response	Description
		The current stop time (hours and minutes) is printed individually after the prompt. Respond with the new stop time.
	X	Remove value and return to OFFP prompt.
- DAYS	d...d	Respond with a new set of days to be used.
		Maximum of seven entries in the range of 1-7. For example, Day 1 = Sunday, Day 2 = Monday.
- COS		Off-hour period Class of Service.
	(UNR)	Unrestricted
	CTD	Conditionally Toll-Denied
	CUN	Conditionally Unrestricted
	FR1	Fully Restricted Class 1
	FR2	Fully Restricted Class 2
	FRE	Fully Restricted
	SRE	Semi-restricted
	TLD	Toll Denied
- TGAR	(0)-15	Trunk Group Access Restriction.
- NCOS	0-99	Network Class of Service.
- ICR	(NO) YES	Incoming Calls are Restricted.
LOCK	(1)-8	Lock period.

LD 88 – If the system is in an off-hour or locked period when a print command is issued, an asterisk appears following the restrictions being used. If lock is in effect, an additional asterisk appears following the lock prompt. The print command allows tenant number to be entered. The status of a tenant SAR group can be printed.

LD 88 – Print command.

Prompt	Response	Description
REQ	PRT	Print.
TYPE	SAR	Scheduled Access Restrictions.
CUST	xx	Customer number.
SPWD	xxxx	Secure data password.
TEN	1-511	Tenant number.
SCRP	0-999	Prompted only if no tenant number is entered.

LD 88 – With SAR, configure the Authcode data block not to automatically generate Authcodes.

Prompt	Response	Description
REQ	NEW	New.
TYPE	AUB	Authcode data block.
CUST	xx	Customer number.
SPWD	xxxx	Secure data password (same password as defined for DISA on a per customer basis in LD 15).
ALEN	1-14	Number of digits in Authcodes.
ACDR	YES NO	Activate CDR for Authcodes (there is no default response).

Prompt	Response	Description
RANR	0-511	RAN route number for Authcode last prompt.
	X	Enter X for no entry.
CLAS	(0)-115	Classcode value assigned to Authcode.
AUTO	NO	Do not automatically generate Authcodes.
		The AUTO prompt appears when NAUT package 63 is equipped and REQ = NEW. The Authcode length must be a minimum of four digits.

LD 88 – Define SAR entries in the Authcode entries data block.

Prompt	Response	Description
REQ	NEW CHG	Add, or change.
TYPE	AUT	Authcode entries data block.
CUST	xx	Customer number.
SPWD	xxxx	Secure data password (same password as defined for DISA on a per customer basis in LD 15).
CODE	xxxx...	Authcode (1-14 digits).
SARC	YES NO	Allow or deny Authcode to be used as the Scheduled Access Restriction (SAR) authorization code.
- SERV		SAR service functions for SARC (the SERV prompt appears if SARC = YES).
	(END) ENA	Enable (Denied) Allowed.
	(LKD) LKA	Lock (Denied) Allowed.

Prompt	Response	Description
	(DSD) DSA	Disable (Denied) Allowed.
	(UND) UNA	Unlock (Denied) Allowed.
		Up to four entries can be made at once.
- SRGP	0-999	Number of SAR group to be defined or changed.
	ALL	Change all SAR groups.
CLAS	(0)-115	Class code value assigned to Authcode. Cycle continues with CODE.
		When type = AUT, enter X to configure the Authcode as an exempt code. When this data is printed, the month the Authcode was deactivated is output. The default is 0 when adding Authcode entries.
	X	Exempt Authcode.

LD 10 – For individual analog (500/2500-type) telephones, respond to the SGRP prompt with the SAR group number (0-999).

LD 11 – For individual display phones, or digital telephones, respond to the SCRP prompt with SAR group number (0-999).

LD 12 – For individual Attendant Consoles, respond to the SGRP prompt with the SAR group number (0-999).

LD 16 – For individual trunk routes, respond to the SGRP prompt with the SAR group number (0-999).

LD 57 – To define Flexible Feature Codes for the SAR disable, SAR enable, SAR lock, and SAR unlock functions, respond to the SADS, SAEN, SALK, and SAUN prompts, respectively, with the appropriate FFCs.

LD 93 – For a tenant, respond to the TYPE prompt with TGEN, Respond to the CUST prompt with the customer number. Respond to the TEN prompt with the tenant number. Respond to the SGRP prompt with the number of the SAR group to be assigned to the tenant.

Feature operation

Use Flexible Feature Codes to apply Scheduled Access Restrictions, as described earlier in this feature description.

Trunk Barring

The Trunk Barring feature provides the option of denying or allowing a direct or modified connection between customer-defined routes.

Trunk Barring works in conjunction with Route Access Restriction Tables (ARTs) defined in LD 16. Trunk Barring is applied on a route basis. The four route categories that Trunk Barring recognizes, and the types of routes in each category, appear in the following table:

Route Category	Route Types
Central Office Trunk (COT)	COT, FEX, WAT
Direct Inward Dialing	DID, DOD
TIE	ATVN, TIE, CAA, CAM, CSA
Other trunk types	ADM, AID, DIC, MDM, PAG, RCD

Operating parameters

When activated in conjunction with the Route Access Restriction Tables, Trunk Barring can prohibit previously allowed connections. Previously restricted connections cannot be lifted or circumvented by Trunk Barring.

Trunk Barring applies to all methods of connecting the trunks (for example, dialing route access, call modification, attendant extension). However, it does not apply to RAN, Music, AWU, or CAS trunks as it is inconsistent with their defined purpose.

Feature interactions

Access Restrictions

Trunk Barring is at the top of the hierarchy for access restrictions.

Attendant-extended calls

When an attendant attempts to extend an Originating Trunk Connection on a barred route, overflow tone is given.

Call Transfer

The originator of a call transfer, unless otherwise restricted, is able to connect to a denied party on a consultation basis. Operating the Transfer key on a BCS telephone or going on hook on an analog (500/2500-type) telephone does not result in a call transfer if the Originating Trunk Connection is barred. The user of a BCS telephone remains connected to the denied party until releasing the connection and returning to the held Originating Trunk Connection. The user of an analog (500/2500-type) telephone is rerung by the Originating Trunk connection when a transfer is attempted and denied.

Call Forwarding

If an Originating Trunk Connection is forwarded to a barred route, it receives the intercept treatment specified in the customer data block.

Conference Calls

The originator of a conference call can only connect to a barred route on a consultation basis. A switchhook flash from an analog (500/2500-type) telephone results in a reestablished connection with the Originating Trunk Connection. The use of a BCS telephone must release the barred connection to return to the Originating Trunk connection or the conference containing the Originating Trunk connection; operating the Conference key on a BCS telephone has not effect. An attendant can return to the Originating Trunk Connection or the conference containing the Originating Trunk Connection by releasing the barred connection. This is done by pressing the RLS DEST key; pressing the Conference key has no effect.

Intercept Treatment/Direct Trunk Access

When an Originating Trunk Connection (OTC) attempts a trunk connection to a route that is restricted by its Access Restricted Table, the connection is not allowed. The intercept treatment specified in the customer data block is applied.

Enhanced Night Service

Any incoming trunk call that is routed by Enhanced Night Service to a telephone from which it is barred will not be connected. Overflow tone (fast busy) will be given to the incoming trunk instead.

Any incoming trunk call that is routed to an outgoing Public Network trunk will be barred if Enhanced Night Service is active. Overflow tone (fast busy) will be given to the incoming trunk instead. This restriction is in addition to the configured trunk barring for the system.

Toll Operator Break In

Trunk Barring results in intercept treatment for all route types that can be barred except Toll Operator Break In.

Feature packaging

This feature requires Trunk Barring (TBAR) package 132.

Feature implementation

In most cases that require barring, only one Access Restriction Table (ART) is necessary. When a new route is created (in LD 16), the default ART defined for that route type is assigned to the route. Use LD 56 to change the ART associated with a route or to handle other nondefault conditions.

LD 56 – Enter or change Trunk Barring parameters.

Prompt	Response	Description
REQ	NEW CHG	Add, or change Trunk Barring parameters.
TYPE	TBAR	Add or change Access Restriction Tables (s) (ARTs).
-ART	1-63	Select ART to add or change.

Prompt	Response	Description
-DENY	yyy yyy	ART numbers denied originating trunk connection (OTC).
	ALL	Deny all ARTs to OTC.
	Xyyy Xyyy	ART numbers allowed to OTC.
TYPE	RART	Change ART number for the route.
-CUST	xx	Customer number.
-ROUT	(0)-127	Route number.
-ART	0-63	ART to assign to route.
TYPE	RCDT	Change the route category default table.
-COT	(0)-63	COT,FEX, and WAT routes are assigned the entered number.
-DID	(0)-63	DID and DOD routes are assigned the entered number.
-TIE	(0)-63	ATVN, CAA, CAM, CSA, and TIE routes are assigned the entered number.
OTH	(0)-63	ADM, AID, DIC, MDM, PAG, and RCD routes are assigned the entered number.

Feature operation

No specific operating procedures are required to use this feature.

System Access Enhancements

System Access Enhancements (SAE) improve the Operations, Administration and Maintenance (OA&M) for System Security and Toll Fraud prevention.

These enhancements strengthen the system security through changes to the following:

- Default Class of Service (CLS)
- Default Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG)
- Call Forward Default Length and Range
- Security Banner at System Login
- Number of Invalid Attempts to LAPW Password in Overlays
- PWD2/PWD1/LAPW Passwords and LAPW Login names
- Problems Determination Tool (PDT) Access Information

Default Class of Service (CLS)

System Access Enhancements provide highly restricted access by defaulting the Class of Service (CLS) to Conditionally Toll Denied (CTD) for all newly configured data. This Class of Service requires users to go through the Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS) to complete a call. Therefore, the possibility of unauthorized toll calls through the system is reduced.

Class of Service (CLS) is defaulted to Conditionally Toll Denied (CTD) in the following Overlays:

- LD 10 – Analog (500/2500-type) Telephone Administration
- LD 11 – Meridian Digital Telephone Administration
- LD 14 – Trunk Data Block (only TIE, CSA, ATVN, FGD, and IDA trunk types default to CLS of CTD)
- LD 16 – Route Data Block, Automatic Trunk Maintenance
- LD 24 – Direct Inward System Access

- LD 27 – ISDN Basic Rate Interface (BRI) Administration (only TIE trunk type defaults to Class of Service (CLS) of Conditionally Toll Denied (CTD))
- LD 88 – Authorization Code

The existing System Access functionality is not impacted by this default change.

Default Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG)

The defaults for Trunk Group Access Restriction (TGAR) and Trunk Access Restriction Group number (TARG) were previously "0". This provided unrestricted toll access after CLS had been checked. System Access Enhancements, however, changes the default TGAR and TARG to "1" in order to automatically block direct access. TGAR is changed from "0" to "1" for the following Overlays:

- LD 10 – Analog (500/2500-type) Telephone Administration
- LD 11 – Meridian Digital Telephone Administration
- LD 14 – Trunk Data Block
- LD 24 – Direct Inward System Access
- LD 27 – ISDN Basic Rate Interface (BRI) Administration
- LD 88 – Authorization Code

TARG is changed from "0" to "1" in the following overlay:

- LD 16 – Route Data Block, Automatic Trunk Maintenance

The existing System Access functionality is not impacted by this enhancement.

Call Forward Default Length and Range

System Access Enhancements lengthens the Call Forward Directory Number to any number of digits in the range of 4-23. The feature also changes the default length to four digits. The Call Forward All Calls/Internal Call Forward (CFW/ICF) feature functionality is modified to have not more than a single CFW/ICF key for a Meridian 1 Proprietary telephone.

Security Banner at System Login

System Access Enhancements (SAE) allows users the option of printing a security banner after login is attempted. To configure this option, the BANR prompt is set to “YES” in LD 17. When BANR is “YES”, a security banner, advising unauthorized users not to attempt login, is printed.

Failed Login Attempt Threshold

Based on the existing implementation of system login, when the Limited Access Password (LAPW) package 164 is equipped, the System Access Enhancements (SAE) strengthens the system security. This is accomplished by limiting the maximum number of invalid login attempts and by performing termination and lock if the number of invalid system password attempts exceeds the defined threshold.

With SAE, in the following overlays, the maximum number of invalid login attempts is limited to the value of the Failed Login Attempt Threshold (FLTH), defined in LD 17:

- LD 15 - Customer Data Block
- LD 17 - Configuration Record 1
- LD 21 - Print Routine 2
- LD 22 - Print Routine 3
- LD 97 - Configuration Record 2

When the number of invalid attempts exceeds the Failed Login Attempt Threshold (FLTH) value, the overlay access is terminated and the current TTY is locked for the LOCK duration, as defined in LD 17.

PWD2/PWD1/LAPW Passwords and LAPW Login names

PWD2, PWD1, and all LAPW passwords were previously stored contiguously in an unencrypted format. With this enhancement, security of PWD2, PWD1, and LAPW usages (if LAPW package 164 is enabled) is enforced by storing contiguously the above system passwords in an encrypted format. By storing passwords in an encrypted format, the random dumping of memory addresses is prevented from revealing passwords.

Problems Determination Tool (PDT) Access Information

System Access Enhancements (SAE) improves the Problems Determination Tool (PDT) by providing a reporting facility for recording this information. Records for valid login, invalid login, logout, PDT initialization, and PDT reboot are produced in a PDT access log file. This file is viewed by both PDT Level 2 and PDT Level 1 users by the new PDT command, RDAACCESS.

Using system management features

The System and Network Management program updates and improves Operations, Administration and Maintenance (OA&M). Meridian Administration Tools (MAT) is a set of tools that provides a Graphical User Interface (GUI) to administer a number of system administration functions.

Two MAT tools provide the following: MAT ESN Administration and MAT Trunks and Routes Administration. They are subdivided into the following:

- Electronic Switched Network (ESN) Database
- Trunk and Route Database
- System Management Base

Electronic Switched Network (ESN) Database

The following overlays support an ESN application on the MAT portfolio:

- LD 86 – Electronic Switched Network 1
- LD 87 – Electronic Switched Network 2
- LD 90 – Electronic Switched Network 3

As the new or changed date/time information is stored at a data group Level, rather than at the individual data element Level, a print function is available in LD 86, LD 87, and LD 90. The data groups are ESN, DGT, NAS, RLB, SCC, and ITGE. This function prints the Last Changed (LCHG) date and time for each data group within the overlays. The printout provides a date/time stamp if any data is changed within the specific data type block. This change is the result of either a NEW, CHG, or OUT command.

Trunk and Route Database

The following overlays support a future Trunk and Route Database application on the Meridian Administration Tools (MAT) portfolio:

- LD 14 – Trunk Data Block
- LD 16 – Route Data Block, Automatic Trunk Maintenance
- LD 20 – Print Routine 1
- LD 21 – Print Routine 2

As the new or changed date/time information is stored at the individual trunk TN Level, a print function is available in LD 14 which prints the Last Changed (LCHG) date and time for all trunk TNs as one data group Level within the overlay. The printout provides a date/time stamp if any data is changed within any trunk data block. This change can be the result of either a NEW, CHG, or OUT command to any trunk data block.

Since the new date information is stored at a data group Level rather than at the individual data element Level, a print function is available in LD 16. This function prints the last changed (LCHG) date for each data group Level within the overlay. The data groups are RDB, ATM, SCH, and NPID.

The input of LD 14 and LD 16 provides the entering of the 16 character DESI field, which can be used to describe the trunk with a name field.

LD 20 and LD 21 print the 16-character designator.

When printing TNB or LTN commands in LD 20, a 16-character designator (DESI) field will be output on the same line as the TN, if it exists.

When printing the Route Data Block (RDB) in LD 21, a 16-character designator (DESI) field will be output on the same line as the route number, if it exists.

System Management Base

Point-to-Point Protocol sessions

Point-to-Point Protocol (PPP) provides remote access to the system. It is established through asynchronous connection to any system Serial Data Interface (SDI) port. Use LD 117 to configure Internet Protocol (IP) addresses for PPP, and defaults are used for all new installation and upgrades.

Three PPP sessions can take place simultaneously.

Multiuser Overlays

The complete list of multiuser overlays are as follows:

- LD 2 – Traffic
- LD 10 – Analog (500/2500-type) Telephone Administration
- LD 11 – Meridian Digital Telephone Administration
- LD 20 – Print Routine 1
- LD 21 – Print Routine 2
- LD 22 – Print Routine 3
- LD 32 – Network and Peripheral Equipment
- LD 44 – Software Audit
- LD 80 – Call Trace
- LD 87 – Electronic Switched Network 2

Overlays are divided into the following categories:

- **Single User-Single Session** – Includes all non-multiuser overlays. Only one of these overlays can load at one time across all sessions.

- **Multiuser-Single Session** – LD 2, LD 32, LD 44, LD 80, and LD 87 are Multiuser-Single Session overlays. Only one copy of these overlays can be loaded at the same time; however, they can run with any other multiuser overlays or one other Single User-Single Session.
- **Multiuser-Multi Session** – LD 10, LD 11, LD 20, LD 21, and LD 22 are Multiuser-Multi Session overlays. Multiple copies of any one of these overlays can be loaded at the same time. They can run with any other multiuser overlays or one other Single User-Single Session overlay.

Simple Network Management Protocol (SNMP) Alarm Agent

In order to provide integrated alarms and Simple Network Management Protocol (SNMP) support from the system, an SNMP Alarm Agent is provided. The SNMP Alarm Agent provides traps for system alarms. These alarms can be fed to an application that supports HP Open View, SNMP support over PPP, or Ethernet. Alarm information, such as the severity, some "simplified" alarm text, and a sequence number, is included in the SNMP traps.

Controlling Call Forward access

Call Forward All Calls (CFW) allows users who are going to be away from their desks to forward their calls to another telephone or location.

This feature is abused when telephones are forwarded to either long distance telephone numbers or Trunk Access Codes, then off-site callers dial the DID extension numbers of these telephones. With the introduction of Remote Call Forward (RCFW), CFW can be abused by forwarding calls to a remote telephone if proper controls are not in place. The following features can help reduce the abuse of Call Forwarding:

- User Selectable Call Redirection
- Call Forward External Deny
- Internal Call Forward
- Call Forward All Calls
- Call Forward to Trunk Access Code

- Call Forward Originating or Forwarded Class of Service
- Remote Call Forward

User Selectable Call Redirection

User Selectable Call Redirection (USCR) allows a user to select the destination for Call Forward No Answer, Busy Hunt, External Call Forward No Answer, and External Hunt. USCR is controlled by Flexible Feature Code, Special Prefix Code, and/or a user key on the multi-line telephone. To use this feature, a Station Control Password is required to prevent abuse.

Since users can direct their calls to external numbers with this feature, this feature must be assigned very selectively to only those users who require the ability to control busy and no answer direction. Unique station control passwords for each telephone are recommended.

Table 16 lists the facilities that can be implemented using USCR, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 16
Implementing USCR

Facility	Overlay and prompts	Print programs
Telephone	LD 10/11 - SETS, SCPW, CLS, USRA, KEY, USR	LD 10, LD 11 by TN or DN LD 22 by DN
Customer	LD 15 - CDB, SPCL, FFCS	LD 21 by CUST or by CFW
Flexible Feature Codes	LD 57 - CODE: USCR, USCR: XXXX	LD 57 by CODE LD 81 by CODE

Call Forward External Deny

Call Forward External Deny (CFXD) restricts call forward from a telephone to an external number thus preventing unauthorized users from placing external calls.

The default value for this feature is Call Forward External Deny (CFXD).

Table 17 lists the facilities that can be implemented using CFXD, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 17
Implementing CFXD

Facility	Overlay and prompts	Print programs
Telephone	LD 10/11 - CLS, CFXD	LD 10/11 by TN LD 81 by CFXA, CFXD

Internal Call Forward

Internal Call Forward (ICF) directs all internal calls to a specified location different from the call forward destination of external calls. An internal call is a station call, DISA call, group call, a call designated as internal over a trunk route, an incoming trunk call using private numbering, or an attendant originated call. To prevent users from call forwarding their telephones to BARS/NARS access codes or trunk access codes and receiving a second dial tone when looping through private networks or accessing the system through DISA when ICF is active, you must disable Call Forward to Trunk Access Codes and Call Forward External must be denied.

Table 18 lists the facilities that can be implemented using ICF, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 18
Implementing ICF

Facility	Overlay and prompts	Print programs
Telephone	LD 10/11 - FTR, KEY, ICF	LD 10,11 by TN LD 81 by ICF
Customer	LD 15 - CFTA	LD 20 by CFW
Flexible Feature Codes	LD 57 - ICFA, ICFD, ICFV	LD 57 by CODE

Call Forward All Calls

Call Forward All Calls (CFW) allows users to forward all calls manually to an external or internal number. To call forward to an external telephone using the CFW feature, Call Forward External Allowed must be enabled on a telephone-by-telephone basis.

The default for CFW is 16 digits, allowing most international calls. However, telephones not requiring external call forward must be restricted to four digits to prevent abuse. Phones permitted external Call Forward must be limited to eight digits.

Table 19 lists the facilities that can be implemented using CFW, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 19
Implementing CFW

Facility	Overlay and prompts	Print programs
Telephone	LD 10/11 - CFW	LD 10/11 by TN LD 81 by CFW

Call Forward to Trunk Access Code

Call Forward to Trunk Access Code (CFTA) restricts DID calls from being forwarded to a Trunk Access Code. This prevents incoming calls from being rerouted to trunking facilities through the system.

Trunk Access Codes must be a minimum of four (six if DN expansion is equipped) digits long. CFW must be restricted to a smaller number of digits than the number of digits in the Trunk Access Code.

Post dialing capabilities can be performed with AC1/AC2 but not with ACOD.

Table 20 lists the facilities that can be implemented using CFTA, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 20
Implementing CFTA

Facility	Overlay and prompts	Print programs
Customer	LD 15 - CFTA	LD 21 by CUST
Route	LD 16 - ACOD	LD 21 by Route
Telephone	LD 10/11 - CFW4	LD 10/11 by TN

Call Forward Originating or Forwarded Class of Service

Call Forward Originating (CFO) or Forwarded Class of Service (CFF) uses the CLS access privileges of the telephone or trunk that originates the call or the telephone that forwards the call. By using the CLS that originates the call and prohibiting that source from making external calls, calls are prevented from being forwarded to an external telephone.

This feature is frequently used in restricting the capabilities of DID trunks in forwarding situations.

Table 21 lists the facilities that can be implemented using CFO or CFF, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 21
Implementing CFO or CFF

Facility	Overlay and prompts	Print programs
Customer	LD 15 – OPT = CFF or CFO CFW	LD 21 by CUST or CFW
Trunk	LD 14 – CLS	LD 20 by TN
Telephone	LD 10/11 – CLS	LD 10/11 by TN

Remote Call Forward

Remote Call Forward (RCFW) allows users to activate and deactivate call forwarding from remote telephones. Users enter codes to activate and deactivate the feature, and must also enter a telephone-specific password. This capability is given to users as required.

Table 22 lists the facilities that can be implemented using RCFW, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 22
Implementing RCFW

Facility	Overlay and prompts	Print programs
Customer	LD 15 - SCPL, FFC	LD 21 by FFC
Flexible Feature Code	LD 57 - CODE, RCFA, RCFD, RCFV	LD 57 by FFC
Telephone	LD 10/11 - SCPW, CFW	LD 10/11 by TN

Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS)

Basic Automatic Route Selection/Network Alternate Route Selection (BARS/NARS) routes outgoing calls over the least expensive facility available at the time the user places a call. Use BARS/NARS features to prevent calls to a specific area code or exchange or to international locations. The following features restrict calling privileges for BARS/NARS:

- North American Numbering Plan
- Supplemental Digit Recognition/Restriction
- Network Class of Service and Facility Restriction Level
- Authorization Code Conditionally Last
- Time-of-Day Routing

- Routing Control
- Incoming Trunk Group Exclusion
- Free Calling Area Screening

Supplemental Digit Recognition/Restriction

Supplemental Digit Recognition (SDRR) causes the system to recognize dialing sequences associated with internal calls to prevent callers from using two trunks to complete an internal call. Internal telephones dial the BARS/NARS access code followed by the public telephone number of another internal telephone. This feature prevents callers from using outgoing COT and incoming DID trunks for internal calls by recognizing predefined dialing sequences.

Supplemental Digit Restriction blocks calls to certain telephone numbers within exchanges, area codes, or country codes. This allows calls to be blocked to prefixes typically associated with pay-per-call, for example, 976.

Table 23 lists the facilities that can be implemented using Supplemental Digit Recognition/Restriction (SDRR), the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 23
Implementing Supplemental Digit Recognition/Restriction

Facility	Overlay and prompts	Print programs
ESN	LD 86 - MXSD	LD 86 by FEAT=ESN
Network translation	LD 90 - DENY, LDID, LDDD	LD 90 by NPA, NXX or SPN

Network Class of Service and Facility Restriction Level

Network Class of Service (NCOS) determines calling privileges for telephones, TIE trunks, DISA directory numbers, and Authcodes for outgoing calls that use BARS/NARS. With NCOS, a Facility Restriction Level (FRL) from 0 to 7 can be assigned to determine access to a route. The FRL of the calling party must be equal to or greater than the FRL of the Route List entry in order to complete the call.

BARS/NARS can be configured to ignore TGARs or to use them. When TGARs are ignored, BARS/NARS assesses the NCOS and the FRL to determine which call facilities are available for a particular call. This configuration allows flexibility in using a given trunk group while forcing users to place calls over less expensive facilities. Trunk availability for each call can be based on the FRL requirements for the number dialed rather than basing it on the TGAR assigned to the calling telephone.

BARS/NARS can be configured to include TGAR assignments in determining how the system can route a call. In this case, NCOS, TGAR, CLS, and FRL are used to determine which call facilities are available to process a particular call.

Table 24 lists the facilities restrictions that can be implemented using NCOS and FRL, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 24
Implementing NCOS and FRL (Part 1 of 2)

Facility	Overlay and prompts	Print programs
Network Control	LD 87 - FEAT = NCTL all prompts	LD 87 FEAT = NCTL by NCOS
Route List Index	LD 86 - FEAT = RLB FRL	LD 86 FEAT = RLB by Route List
Authcode	LD 88 - TYPE = AUT CODE, NCOS	LD 88 TYPE = AUT by Authcode
Telephones	LD 10 and LD 11 - NCOS	LD 10/11 by TN LD 81 by NCOS

Table 24
Implementing NCOS and FRL (Part 2 of 2)

Facility	Overlay and prompts	Print programs
Trunk	LD 14 - NCOS	LD 20 by TN
Customer	LD 15 - NET	LD 21 by NET
SSC list	LD 18 - NCOS	LD 20 by SCL
DISA	LD 24 - NCOS	LD 24 by DISA directory number

Authorization Code Conditionally Last Network Authorization Codes

Network Authorization Codes (NAUT) can be configured to prompt users who fail to meet the minimum FRL requirement to enter an Authcode to complete a call. This control provides another Level of security by requiring all callers placing calls to international locations or selected area codes, for example, to enter an Authcode.

Table 25 lists the facilities that can be implemented using NAUT, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 25
Implementing NAUT

Facility	Overlay and prompts	Print programs
Route List Index	LD 86 - FEAT = RLB, MFRL	LD 86 FEAT = RLB by Route List Index
Network Control	LD 87 - FEAT = NCTL, NCOS, FRL	LD 87 by NCOS
Authcode	LD 88 - TYPE = AUT, CODE, NCOS, RANR	LD 88 TYPE = AUT by Authcode
Telephones	LD 10 and LD 11 - NCOS	LD 10/11 by TN LD 81 by NCOS
Trunk	LD 14 - NCOS	LD 20 by TN
Customer	LD 15 - NET	LD 21 by NET
SSC list	LD 18 - NCOS	LD 20 by SCL
DISA	LD 24 - NCOS	LD 24 by DISA directory number

Time-of-Day Routing

Each entry in a route list is assigned to a Time-of-Day (TOD) schedule that specifies the hours that a particular entry can be accessed.

With this feature employees can be restricted from calling locations they have no need to call for business purposes at certain hours. Because the majority of toll fraud calls occur on holidays or after normal business hours, use this feature to deny access to routes supporting calls to international locations or to the 809 area code after hours.

Table 26 lists the facilities that can be implemented using TOD, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 26
Implementing TOD

Facility	Overlay and prompts	Print programs
ESN	LD 86 - FEAT = ESN, TODS	LD 86 FEAT = ESN
Route List Index	LD 86 - FEAT = RLB, TOD	LD 86 FEAT = RLB by Route List Index

Routing Control

Routing Control (RTCL) uses Time of Day (TOD) schedule 7 as an alternate TOD to modify user's network access capabilities automatically for a defined time frame each day and/or on weekends. In addition, a key can also be assigned on the attendant console that will manually activate/deactivate RTCL.

Activating this feature prevents people from accessing unattended telephones after hours to place unauthorized calls. However, Authcodes are not subject to the alternate NCOS assignments imposed through RTCL. When users enter valid Authcodes, they are provided with the Network Classes of Service assigned to the Authcodes for the duration of the call.

Table 27 on page 66 lists the facilities that can be implemented using RTCL, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 27
Implementing RTCL (Part 1 of 2)

Facility	Overlay and prompts	Print programs
ESN	LD 87 - FEAT = ESN, TODS 7, RTCL, NMAP, ETOD	LD 87 FEAT = ESN
Attendant	LD 12 - KEY = RTC	LD 20 by TN

Table 27
Implementing RTCL (Part 2 of 2)

Facility	Overlay and prompts	Print programs
Network Control	LD 87 - FEAT = NCTL NCOS	LD 87 by NCOS
Telephones	LD 10 and LD 11 - NCOS	LD 10/11 by TN LD 81 by NCOS
Trunk	LD 14 - NCOS	LD 20 by TN
Customer	LD 15 - NET	LD 21 by NET

Incoming Trunk Group Exclusion

Incoming Trunk Group Exclusion (ITGE) blocks network calls originating on TIE trunks from reaching certain destinations. Each TIE route is associated with a table that defines the dialing sequences allowed for calls originated on that TIE route.

This feature prevents users from calling locations they do not need to reach for business purposes and keeps them from attempting to circumvent restrictions that are imposed at their local PBX. It also helps prohibit a technique called “looping” that hackers use to cover their tracks when accessing a network for toll fraud purposes.

Table 28 lists the facilities that can be implemented using ITGE, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 28
Implementing ITGE

Facility	Overlay and prompts	Print programs
ESN	LD 86 - FEAT = ESN, MXIX	LD 87 FEAT = ESN
ITGE	LD 86 - FEAT = ITGE all prompts	LD 86 FEAT = ITGE by ITGE Index
Network translation	LD 90 - FEAT = NET ITED, ITEI	LD 90 FEAT = NET by NPA, NXX, SPN, or LOC

Free Calling Area Screening

Free Calling Area Screening (FCAS) provides full six digit screening to determine the route choice for completion of off-net calls. With FCAS, calls can be allowed to certain area codes and restricted from other area codes within the free calling area surrounding a particular on-net location.

FCAS tables define the NPA codes and NXX codes used to screen calls. Each table is referenced by an FCI number that is assigned to a route; 0 indicates that the FCAS feature is not enabled for that route.

Table 29 on page 69 lists the facilities that can be implemented using FCAS, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 29
Implementing FCAS

Facility	Overlay and prompts	Print programs
Route List Index	LD 86 - FCI	LD 88 FEAT = RLB by Route List Index
Free Calling Area Screening	LD87 - FCAS (allow, deny)	LD 87 - FEAT = FCAS
FNP		
Truncated CDR		

Controlling Direct Inward System Access

Direct Inward System Access (DISA) allows employees, when they are off-site, to place calls to internal extensions and to private and public network locations through the company PBX. Access to the system DISA feature is usually through dedicated trunks such as 1-800 service CO trunks. These trunks can be programmed to auto-terminate at a DISA directory number. DISA is not recommended for DID trunks.

Table 30 lists the facilities that can be implemented using DISA, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 30
Implementing DISA

Facility	Overlay and prompts	Print programs
Customer Data Block	LD 15 - SPWD	LD 21 by SDP, PWD2
DISA directory number	LD 24 - SPWD, DN, SCOD, AUTR, TGAR, NCOS, COS	LD 24 by DISA Block

A DISA directory number must be restricted by Authcodes and Security codes to protect access to the system.

DISA can also be controlled using a combination of Routing Control (RTCL) and NCOS assignments to limit the weekend and evening access to this feature. Assigning unique NCOS Levels to either the DISA directory number or Authcodes used by DISA reduces the access capability of the NCOS by lowering it to a more restricted Level using RTCL. Refer to "Routing Control" on page 66 for configuration details.

To help prevent unauthorized persons from using DISA features, activate the following:

- Security Code
- Authorization Code
- Service restrictions

These features can be used alone or in combination with each other to provide the level of security that necessary for that telecommunications facility.

Security Code

The system can be programmed to require a Security Code (SCOD) so that when the system answers a DISA call, callers must enter the SCOD assigned to the DISA directory number before they can gain access to the system. This SCOD can be from 1 to 8 digits long. The SCOD can be used in conjunction with an Authcode if desired.

Table 31 lists the facilities that can be implemented using the SCOD feature, the programs and prompts to implement the feature, and the programs to print information about the feature.

Table 31
Implementing SCOD

Facility	Overlay and prompts	Print programs
DISA directory number	LD 24 - SCOD	LD 24 - DISA Block

Authorization Code

DISA callers can be required to enter an Authorization Code (Authcode) before they can gain access to system facilities. Assign Authcodes that are from 1 to 14 digits long.

If DISA is not configures to require an Authcode, users can still enter such a code by dialing SPRE + 6 followed by a valid Authcode. Either way, users take on the CLS, TGAR, and NCOS assigned to the Authcode entered. Users' calling capabilities are then based on the service restrictions assigned to the Authcode. Authcodes can be used in conjunction with Security Codes.

Refer to "Authorization Code" on page 28 for information about how to assign Authcodes to DISA.

Service restrictions

A CLS, TGAR, and NCOS can be assigned to a DISA directory number to restrict access through DISA. When the system accepts calls without requiring callers to enter Authcodes, they automatically receive the assigned DISA directory number calling privileges.

Refer to "Class of Service" on page 20, "Trunk Group Access Restrictions" on page 23, and "Network Class of Service and Facility Restriction Level" on page 63 for information about assigning these restrictions to the DISA directory number.

Controlling Multi-Tenant Services

Multi-Tenant Services (TENS) allow a customer to divide its services and resources into subgroups known as tenants. Access to tenants, attendant consoles, and trunk routes can be configured so that tenants have private use of some facilities, share some facilities, or are denied access to other facilities. All tenants share the numbering plan and features of the customer. TENS must be protected with security features to help prevent unauthorized use of these facilities. Restrictions must be implemented to control:

- Tenant-to-tenant access
- Tenant-to-route access
- Console Presentation Group assignment

Tenant-to-Tenant Access

A tenant's relationship with other tenants of the same customer is defined by Tenant-to-Tenant Access (TACC). A tenant can be configured to allow direct internal call access to some or all tenants of the same customer. Likewise, a tenant can be denied direct access to other tenants.

Table 32 lists the facilities that can be implemented using TACC, the programs and prompts to implement them, and the programs to print information about the feature.

Table 32
Implementing TACC

Facility	Overlay and prompts	Print programs
Tenant-to-tenant access	LD 93 - TACC	LD 93 Define Tenant to Tenant access

Tenant-to-Route Access

Each customer can have a maximum of 128 trunk routes. Each tenant can share or have private access to any or all of these routes. Tenant-to-Route Access (RACC) applies only to outgoing calls.

Table 33 lists the facilities that can be implemented using RACC, the programs and prompts used to implement them, and the programs to print information about the feature.

Table 33
Implementing RACC

Facility	Overlay and prompts	Print programs
Tenant-to-Route access	LD 93 - RACC	LD 93 Define Tenant to Route access

Console Presentation Group (CPG) assignment

Attendant consoles are placed into Console Presentation Groups (CPGs) that are associated with specific tenants and specific incoming trunk routes. The CPG range is from 0 to 63. All attendant consoles configured for a customer are automatically members of CPG 0. Other CPGs are defined to fit tenant requirements using the configuration program.

Table 34 lists the facilities that can be implemented using CPG, the programs and prompts used to implement them, and the programs to print information about the feature.

Table 34
Implementing CPG

Facility	Overlay and prompts	Print programs
Console Presentation Group	LD 93 - CPG, NIT1 to NIT4	LD 93 CPG

Meridian Mail security features

Contents

This section contains information on the following topics:

Introduction. 76

Controlling mailbox features 76

- Permission/restriction tables. 77
- Permission/restriction tables. 77
- Controlling User Extension Dialing. 78
- Controlling Express Messaging. 78
- Controlling Operator Revert. 78
- Controlling Call Sender. 79

Controlling Voice Menu/Thru-dialer. 79

Fax on Demand. 79

Controlling mailbox access. 79

- Invalid Log-on Attempts. 80
- Mailbox Password Change 80
- Secured Messaging. 81

Controlling the administration terminal. 82

- Hardware based remote access restriction. 82
- Switchroom access. 83

Controlling Outcalling. 83

Controlling the Meridian Mail virtual agents. 84

Controlling upgrades. 84

Controlling AMIS networking. 85

Reference list

The following are the references in this section:

- *Meridian Mail system administration guide* (553-7001-302)
- *Meridian Mail Fax on Demand Application Guide* (553-7001-327)

Introduction

This chapter describes Meridian Mail security features and how to implement them. This is done by limiting and controlling access to Meridian Mail through the following:

- controlling mailbox features (Permission/Restriction Tables)
- controlling External Caller Dialing and Fax on Demand
- controlling Secured Messaging
- controlling Classes of Service
- controlling Voice Menus/Thru-dialer
- controlling mailbox access
- controlling the administration terminal
- controlling outcalling
- controlling Meridian Mail virtual agents
- controlling upgrades
- controlling Audio Messaging Interchange Specification (AMIS) networking

Because Meridian Mail features vary from one release to another, any differences between the releases regarding operation and security implementation will be discussed. For additional information on Meridian Mail features and how to implement them, refer to *Meridian Mail system administration guide* (553-7001-302).

Controlling mailbox features

Control of Meridian mailbox features is accomplished by the following:

- Restriction tables

- Permission/restriction tables
- Call Answering Thru-dial, User Extension Dialing Express Messaging, Custom Operator Revert, and Call Sender

Permission/restriction tables

In Meridian Mail software, both restriction and permission codes are grouped into four tables according to type. Each table consists of ten permission and restriction codes, one to five digits in length.

Default names for the four user-definable tables are: **On-Switch**, **Local**, **Long Distance 1**, and **Long Distance 2**. These table names can be changed by the user.

These tables provide greater flexibility in allowing some users access to local and long distance numbers while restricting other users. These tables must include BARS/NARS access codes, trunk access codes, special prefix codes, and any extensions such as the CEO's or company president's.

Make sure that long distance Thru-dialing is blocked if the company requires Thru-dialing to local numbers. Hackers use outbound trunks to access operator and long distance services.

If no table is applied, there are no restrictions on placing calls. Systems are shipped with Thru-dial blocked in all permission/restriction tables. The default table assigned to Thru-dial features is **Local**. After system installation, tables must be redefined to permit all forms of Thru-dial.

In multicustomer applications, all customers share the same four sets of permission/restriction tables. The system matches the numbers dialed on Thru-dial applications against the permission/restriction table assigned. The most complete match is applied.

After tables are defined, they are assigned to Thru-dialing features such as Call Answering/Express Messaging Thru-dial, Custom (operator) Revert, and Extension Dialing.

Example

In the permission/restriction table, the following codes are specified:

Restrict	1	2	3	4	5	6	7	8	9	0

Permit: 91800 _____ _____ _____ _____

Only calls beginning with "9 1 800" are permitted in this table. By default, any number not defined as either a permission or restriction entry is considered permitted. If a value is defined as both the permission and restriction entries, it is considered permitted.

Call Answering Thru-dial

Thru-dial allows callers to dial another extension number or a valid telephone number once Meridian Mail answers. Callers dial 0 followed by an extension number, valid access code, and telephone number and are routed to the numbers dialed. The permission/restriction table associated with this function is effective systemwide and is assigned on the **Voice Security Options** screen.

Controlling User Extension Dialing

User Extension Dialing is a Thru-dialer that allows users logged into their mailboxes to reach other extensions. If a hacker logs into a mailbox, the hacker has access to the Thru-dialing capabilities intended for the user of that mailbox. A permission/restriction table is assigned to each mailbox on the **Modify User** screen.

Controlling Express Messaging

Express Messaging allows users to access Meridian Mail directly without having to call a user's directory number and wait to be forwarded. A permission/restriction table is applied to this feature to control the numbers that can be dialed by users during Express Messaging sessions.

Controlling Operator Revert

Operator Revert allows callers to revert to a predefined extension number by dialing 0 during the personal greeting or after leaving a message. This extension number is called an Operator Revert DN. Users are allowed to set their own Operator Revert DNs. Permission/restriction tables are assigned for each mailbox using the **Modify User** screen.

Controlling Call Sender

External Call Sender is applicable only if Meridian Networking is installed. This feature allows a Meridian Mail user to immediately call back the sender of a read message by pressing 9. A permission/restriction table can be applied to this feature to identify the call sender extension.

Controlling Voice Menu/Thru-dialer

Voice Menu/Thru-dialer allows the Thru-dial feature to be defined as either a stand-alone server or an option within a Voice Menu. This feature allows incoming callers accessing a Voice Menu to dial another extension or telephone number when the option is accessed. When properly configured, unauthorized access to long distance facilities through Voice Menu/Thru-dialer is prevented.

Thru-dialers can assign custom permission/restriction tables or one of the permission/restriction tables that are defined for outcalling and mailboxes.

If calls require Thru-dialing outside the system for a particular Thru-dialer, that Thru-dialer can be protected by requesting users to enter a password from 4 to 16 digits in length.

Make sure that Automated Attendant features in voice menus are protected with adequate permission/restriction tables as well. In-bound 1-800 numbers terminating on an automated attendant are hackers' favorite targets.

Fax on Demand

Refer to *Meridian Mail Fax on Demand Application Guide* (553-7001-327) for information on implementing security for Fax on Demand.

Controlling mailbox access

To minimize unauthorized use of the company's mailboxes, change the mailbox password frequently and disable any unused mailboxes. The following security features are available to assist in preventing unauthorized use of Meridian Mail:

- Invalid Log-on Attempts

- Mailbox Password Change
- Secured Messaging

Enable and define these features for all mailboxes using the administration terminal **Voice Security Option** screen.

Invalid Log-on Attempts

The Invalid Log-on Attempts feature helps prevent unauthorized persons from entering one password after another until they gain access to a mailbox. This feature defines the number of times, within a range of one to nine, a caller can enter an invalid log-on password for a mailbox before the system disables the mailbox. Once the mailbox is disabled, only the system administrator can re-enable it at the administration terminal. When a mailbox is disabled, Meridian Mail still takes and stores incoming messages but does not permit log-on.

The administrator can define the number of invalid log-on attempts per mailbox as well as the number of invalid log-on attempts per session.

Mailbox Password Change

Password Change allows a minimum password length to be established for all mailboxes. The password length must be from 4 to 16 digits long.

The number of days that a password is valid can be set from 0 to 90. If a user does not change a mailbox password within the specified time, the mailbox continues to receive messages but the user cannot retrieve them until the password is changed.

A parameter can be set that defines the number of password changes required before users can reuse previously defined passwords. This parameter can range from 1 to 5.

A password expiring warning can be provided to users when they log on to Meridian Mail. The warning tells users the number of days before their password expires. This message can be sent to the user anytime from 1 to 60 days before the password expires.

Note: If changing password size and turning off the password change option, be sure to define adequate time for users to establish their new passwords before the old password expires.

Adopt the following password management practices to avoid or minimize mailbox abuse:

- Avoid simple passwords or those that are derived from personal information such as social security number, home telephone number, birth dates, and so on.
- Force password changes on mailboxes every 60 to 90 days.
- Require users to change passwords several times (five minimum) before they can repeat previously used passwords.
- Require that passwords be a minimum of six digits long.
- Don’t use default passwords when setting up mailboxes. The administrator must choose a unique six character password when adding a mailbox.
- Force users off the system after three invalid log-in attempts.
- Delete all unused mailboxes, unused guest mailboxes, and mailboxes of terminated employees.

Secured Messaging

Secured Messaging is installed at the factory and prohibits external calls from logging on to Meridian Mail and retrieving messages. This eliminates the possibility of external hackers gaining access to a mailbox. Users can only retrieve messages by calling from within the system. Once enabled, this feature cannot be disabled without completely reinstalling the software.

Controlling the administration terminal

The system administration terminal default password is ADMINPWD. This password must be changed on a regular basis every 60 to 90 days and when somebody having the Meridian Mail administrator password leaves the company or the distributor. The administrator must change the password at the first log in. Each time an administrator password is changed, a System Event and Error Report (SEER) is printed to indicate the change. A SEER is also generated every time there is an incorrect log-on attempt at any password Level. This notifies the administrator of an attempt to breech the system security.

The administrator must investigate system security and overall system status when the following occurs:

- the Administrator password no longer provides access because it has been changed or locked out.
- a SEER indicates that the administrator password was changed.
- a SEER indicates a failed administrative log-on attempt has occurred.

If the Multiple Administration Terminal feature is installed, the Meridian Mail system can support a maximum of four administration terminals with user administration capability. Make sure that passwords on these terminals are unique. These passwords must be changed on a regular basis and must coincide with the password changes of the main administration terminal.

Hardware based remote access restriction

Meridian Mail is configured with an A/B box between the terminal and the modem. With the switch set to modem, the system can be accessed remotely. With the switch set to terminal, remote access is disabled. The A/B box must be manually switched at the site. To prevent unauthorized access, the switch must not be left set to the modem setting unless there is a valid reason to do so. In addition, if the system is equipped with AdminPlus configured for a remote device, disable remote access from a remote AdminPlus terminal when this terminal is not in use.

Switchroom access

The same switchroom access precautions exercised for a system PBX must be in place for Meridian Mail. The equipment is usually stored in the same room and, with new installations, the same cabinet.

Controlling Outcalling

The Outcalling feature is really two features: Remote Notification and Message Delivery to Non-users.

Remote Notification provides message notification and delivery to a Meridian Mail user at a remote telephone number such as a pager, car phone, or home telephone. Users must enter the correct mailbox and password when logging on to Meridian Mail before they can retrieve messages. They can change Remote Notification parameters from an off-site location by logging on to Meridian Mail and accessing a special mailbox option menu.

Message Delivery to Non-users delivers messages to people who do not have a Meridian Mail mailbox. Meridian Mail users first define non-user telephone numbers for message delivery and then compose a message in the normal manner. After users enter the SEND command, Meridian Mail dials target numbers and delivers the message when it detects voice, or when the non-user presses 2, if prompted. After the system plays a message, non-users can record a reply and forward it to the sender. The reply message is automatically deposited in the sender's mailbox.

A different dialing permission/restriction table can be assigned for Remote Notification and Delivery to Non-user for each mailbox. The default for these two features is **Disabled** using the **Local** permission/restriction table.

Besides defining restriction/permission codes for these features, the following can also be defined:

- the number of attempts Meridian Mail makes to notify a user of a waiting message
- the interval between attempts
- the maximum number of Remote Notification retry attempts
- the times of day Meridian Mail can deliver messages to a non-user

- the number of attempts Meridian Mail makes to deliver messages to a non-user
- the number of times to play a message to a non-user
- the type of Dual Tone Multifrequency (DTMF) confirmation tone
- an audit trail

Controlling the Meridian Mail virtual agents

Another line of defense against toll fraud through Meridian Mail is to restrict the access privileges of Automatic Call Distribution (ACD) virtual agents that serve Meridian Mail ports. Each Meridian Mail ACD agent must be restricted to allow only calls that are required by the applications running the Meridian Mail system. The access privileges of these agents must restrict access to outbound trunk groups that never need to be accessed by Meridian Mail.

The administrator can restrict Meridian Mail ports by assigning the NCOS, TGAR, and CLS that best meet the company's security and user needs. Refer to "Network Class of Service and Facility Restriction Level" on page 63, "Trunk Group Access Restrictions" on page 23, and "Class of Service" on page 20.

When setting access privileges for these agents, keep in mind that there can be legitimate Meridian Mail applications that need to make toll calls. Some of these are Delivery to Non-users, Networking, and Remote Notification with paging.

Controlling upgrades

After an upgrade, it is recommended that an audit of security parameters be carried out to ensure that the appropriate permission/restriction table is assigned to any new feature. This is also true if implementing a feature that was not used in a previous release.

Controlling AMIS networking

The Audio Messaging Interchange Specification (AMIS) networking protocol is an industry standard that allows users of third-party voice messaging systems to exchange voice messages. Meridian Mail users can send voice messages to users of other voice messaging systems from other AMIS sites and reply to these messages using standard Meridian Mail functionality. The AMIS open access design allows anyone who has access to AMIS to send messages without the need for prearranged passwords, site definitions, or specialized hardware.

Make sure that AMIS programming restricts unauthorized access in the voice menu, Thru-dial, or AMIS networking information screens.

System access security features

Contents

This section contains information on the following topics:

Controlling access to administration programs. 87
Password management 88
Recommended password management practices. 89
Program access control. 92
Audit Trail review. 93
History File review. 94
Controlling access to the system. 95
System administration port security. 95
Switchroom security. 96
Network facilities security. 96
Problem Determination Tool (PDT) access. 97
Controlling access to system Application Processors. 103

Controlling access to administration programs

Administration programs (overlays) are used to configure the customer database and conduct day-to-day routine system administration functions. Unauthorized access to these programs can make the system vulnerable to abuse and performance degradation or failure. For this reason, strict security must be implemented to help prevent unauthorized system access. This is accomplished with:

- Password management
- Program access control

- Audit Trail review
- History File review

Password management

Proper password selection and frequent password changes provide an important safeguard against unauthorized system access.

Two types of passwords allow access to database configuration and maintenance programs:

- level 1 passwords
- level 2 passwords

Use digits from 0 to 9 and alphabetic characters A through Z, to form a password. Passwords are case-sensitive.

Level 1 password

The administrator can use the level 1 password to log on to the PBX to change the configuration database. Level 1 passwords cannot change level 1 passwords, level 2 passwords or the secure data password associated with assigning Authorization Codes (Authcodes) and DISA parameters (if defined).

Table 35 lists the facility that can be implemented using a level 1 password, the programs and prompts to implement the password, and the programs to print information about the password.

Table 35
Implementing a level 1 password

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - PWD2, NPW1	LD 22 by Passwords (must know level 2 PWD2-password)
	LD 17 - LNAME_OPTION LOGIN_NAME: 0-9, A-Z	LD 22 by AUDT

Level 2 password

The level 2 password provides all privileges of the level 1 password. It also allows the level 1 and level 2 passwords, as well as the secure data password, to be changed.

When accessing the system using a Limited Access Password, the Limited Access to Overlays feature can be configured to require a user name to be entered with up to 11 alphanumeric characters.
The user name can only be configured by the administrator using the level 2 password.

Table 36 lists the facility that can be implemented using a level 2 password, the programs and prompts to implement the password, and the programs to print information about the password.

Table 36
Implementing a level 2 Password

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - PWD2, NPW2	LD 22 by Passwords (must know level 2 PWD2-password)
	LD 17 - LNAME_OPTION: LOGIN_NAME: 0-9 A-Z	LD 22 by AUDT

Recommended password management practices

Nortel Networks recommends that the following password management practices be used to avoid or minimize unauthorized access to the administration terminal:

- Avoid simple passwords or those that are derived from personal information such as social security number, home telephone number, birth dates, and family names.
- Change the password every 60 to 90 days.
- Change a password several times (a minimum of five times) before repeating a previously used password.

- system passwords must be a minimum of eight characters in length and alphanumeric. A longer password provides greater security.
- The password must be changed during installation and again at system cutover.
- Invalid log-in thresholds must be set to 3; manual initialization will override the lock-out time limit defined for invalid attempts. This must be programmed. The default = NO.
- Change the system password when anyone knowing a system password leaves the company.

Single Terminal Access

The Single Terminal Access (STA) feature reduces the number of physical devices needed to administer and maintain a system and its associated subsystems.

When the user intends to switch to another system, a mechanism for ending the original session is provided in the STA application through a user-determined log-out sequence. This sequence is specified in the database with each STA port. This sequence is automatically be sent to the destination system by the application to prevent users from leaving a session open in the background without logging out.

If the log-out sequence is not programmed, or is programmed incorrectly, the user could leave a program open in the background, and the system could be subject to unauthorized access.

The STA master terminal will use the configured log-out sequences to automatically exit from the active and existing background sessions when the modem connection for the terminal experiences carrier drops out.

A password is required before the user can enter NEW or CHANGE to configure an STA port. This process is designed to protect the STA port from unauthorized alteration.

Table 37 lists the facility that can be implemented to configure STA, the programs and prompts to implement single terminal access, and the programs to print information about single terminal access.

Table 37
Implementing single terminal access

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - ADAN, STA, TTY, CTYP, GRP, DNUM, ADMIN_PORT, LANGUAGE, ADDITIONAL_PORT	LD 22 by CFN or ADAN

Multiuser log-in

Multiuser log-in allows up to five users to simultaneously log into a system PBX to load and execute overlays. A sixth overlay can be running at midnight or in the background. This feature supports only the following:

- sets administration
- maintenance
- midnight routines
- background routines
- attendant administration

The History File includes separate Log Files for each configured TTY port to record each technician's maintenance and administration activities.

A user can be forced to log off a terminal if a level 2 or Limited Access Password user logs in to the PBX. A monitor command allows a logged in user to monitor the input/output activities of a different local or remote terminal.

Table 38 lists the facility that can be implemented using a level 2 password and multiuser log-in, the programs and prompts to implement the password, and the programs to print information about the password.

Table 38
Implementing level 2 password and multiuser log-in

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - PWD2, LAPW, TLOG, SIZE MULTI-USER ON(OFF)	LD 22 by CFN or LAPW LD22 by CFN or LAPW

Program access control

The Limited Access to Overlays feature, controlled through Limited Access Password (LAPW), provides a greater degree of control of password assignment and program access. It also enhances tracking of PBX access. This feature provides additional security by allowing up to 100 LAPW passwords to be defined per system. The LAPW passwords can be 4 to 16 alphanumeric characters in length.

In addition to the log-in time, name, and password, the LAPW Audit Trail provides a time stamp indicating when the user logged out. When accessing the system using LAPW, the Limited Access to Overlays feature can be configured to require a user to enter a user name with up to 11 alphanumeric characters.

Access to specific programs can be defined for each password and a Print Only capability specified. An Audit Trail can be configured to record the date, time, password used, and programs accessed. The system performs the following actions:

- monitors failed log-on attempts
- compares the number of attempts with a predefined threshold
- locks the entry port if the threshold is exceeded

The system reports lock-out conditions on all terminals and provides a special report to the next administrator who logs on.

Table 39 lists the facility that can be implemented using Limited Access to Overlays programs, the prompts used to implement the feature, and the programs to print information about the feature.

Table 39
Implementing the Limited Access to Overlays feature

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - LAPW, PWnn, OVLA, CUST, TEN, OPT = CFPD(A), LLCA(D), PROA(D), PSCD(A), HOST, FLTH, LOCK, AUDT, SIZE, INIT	LD 22 by CFN or LAPW

Audit Trail review

The Audit Trail stores system activities messages in memory. The stored information can be accessed using a system terminal or a remote device. The information can be printed.

Make sure that the file is large enough to hold all possible entries. Increase the size if necessary.

INIT = YES indicates that a manual initialization is allowed to reset a port locked out due to invalid log-on attempts. If ACD reports are run, this INIT feature will interrupt reports and provide incomplete statistics.

The Audit Trail for Limited Access Password (LAPWs) includes time stamps that indicate when users logged out.

Table 40 lists the facility, shows the program and prompts used to implement the Audit Trail feature, and the program used to print information about the feature.

Table 40
Implementing the Audit Trail

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - AUDT, SIZE, INIT	LD 22 by AUDT or LD 22 by CFN

History File review

The History File stores system messages in memory. The stored information is accessed by using a system terminal or a remote device. The information can be printed.

Specify the types of information to be stored in the History File. This information includes the following:

- maintenance messages (MTC),
- service change activity (SCH),
- customer service change activity (CSC), and
- software error messages (BUG).

Selectively view the History File using the VHST command. This command permits the following actions:

- search forward
- repeat the last search
- go up or down
- define the next or previous number of lines to display
- display lines from the current location to the bottom of the file
- search on a string of up to 12 characters

A Traffic Log file can be created separate from the History File.

Table 41 lists facilities that can be implemented using the History File, programs and prompts to implement the feature, and programs to print information about the feature.

Table 41
Implementing the History File

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB, HIST, USER ADAN SIZE	LD 22 CFN or ADAN

Controlling access to the system

To limit unauthorized functional and physical access to the system and its network connections, provide the following:

- System administration port security
- Switchroom security
- Network facilities security
- Problem Determination Tool (PDT) access

System administration port security

Remote system administration allows PBX technicians to access the system using maintenance modems or the on-site terminal. This allows them to adjust and troubleshoot system hardware and software components. however, unauthorized users can also access the system remotely, alter the system configuration, steal services, and degrade system performance.

Unauthorized users have been known to dial into the remote access port, break the password, and reprogram system memory to allow international calls, enable the DISA feature, turn off Call Detail Recording (CDR), traffic, and history reports, and either eliminate the need for Authcodes or create new ones.

Ports defined as TTY or PRT are controlled by counters monitoring invalid characters. Ports disabled due to invalid characters can be automatically enabled after 4 minutes. Disabled ports can be enabled a maximum of three times in 30 minutes. If a port is disabled four times in 30 minutes, it requires manual enabling.

Access to the system communication ports can be limited with passwords. Refer to "Password management" on page 88.

Switchroom security

If a switchroom is not secure, this permits access by unauthorized users to all the system resources. Their activities can range from turning off printer and CDR processors to removing cards from the PBX and rendering the system inoperable. Follow these security procedures to minimize this risk:

- Limit access to the switchroom to authorized personnel only.
- Require distributor and telephone company personnel to sign in and out and provide identification, if necessary.
- Control, document, and audit major changes to system configuration.
- Require personnel to sign out parts and equipment.
- Store printouts of system configurations and databases in a secure, locked area.
- Do not post passwords or Trunk Access Codes in the switchroom.
- Keep the switchroom and telephone equipment closets locked.

Network facilities security

Network security is just as important as switchroom security. For example, unsecured facilities can be accessed by a lineman using a test terminal to place unauthorized calls without these calls being detected by the PBX and recorded by the CDR.

Follow these security procedures to minimize this risk of abuse:

- Secure the telephone company access point, individual distribution frame location, and the Main Distribution Frame (MDF).

- Avoid locating Intermediate Distribution Frames (IDF) in janitorial, electrical, and supply closets whenever possible. Limit access when colocation is unavoidable.
- Document existing outside and inside cable plans and update these records as service changes are made.
- Where cable plan records do not exist, consider hiring an independent consultant to verify and document the cable plan.
- Maintain and document all moves and changes Eliminate all out-of-service cross connects if not using the Automatic Set Relocation feature.
- Encase and lock building entry terminals and secure manholes.
- Avoid posting cable documentation in the IDF.
- Keep cable plant documentation in at least two separate secure locations.
- Verify terminal connections against cable plant/system records, and resolve all differences.
- Audit the entire system, ensuring that all cable, telephone company, telephone, and PBX records are accurate.

Problem Determination Tool (PDT) access

Problem Determination Tool (PDT) access is password protected. Level 2 PDT users, usually administrators, can change level 1 and level 2 PDT passwords.

For a new system installation and for an upgrade, the system level 1 and 2 passwords are hard coded from previous issues of the software.

For previous issues of software, passwords could be changed by using patch MPLR13326. For an upgrade, if the password was changed previously, it does not need to be changed for Release 25.40; the password only needs to be reset.

To change the level 1 and 2 passwords for a new system installation, or to upgrade from a previous issue of software where the level 1 and 2 passwords were NOT changed previously:

- Follow the steps in “Changing the password” on page 98.
- After the password has been changed, follow the steps in “Resetting the Passwords” on page 99.

To reset a forgotten password, or to upgrade from previous issue of software where the level 1 and 2 passwords were changed previously:

- Follow the steps in “Resetting the Passwords” on page 99.

CAUTION
As soon as the temporary password is no longer required, remove the install disk or return faceplate switches to the original position. If a reboot or INI occurs while the system is in the temporary password condition, large switches may come up in install mode or Option 11 may come up in an error state.
If this occurs, remove the install disk or reset the faceplate switches to the original position and follow with an INI.

Changing the password

For CPP machines

Passwords can only be changed on the active side when the system is joined. If the system is split, the passwords on either side can be changed. However, when the system is joined, the active side will overwrite the inactive side PDT passwords with the active side PDT passwords

For Option 11C machines with IP Expansion

The PDT passwords can only be modified on the main cabinet. All expansion cabinets will use the main cabinet's PDT passwords.

Use the following procedure to change one or both of the PDT passwords.

Procedure 1
Change one or both PDT passwords

1. Enter PDT using the current level 2 password.
2. At the pdt prompt, type ***passwd***.
3. Enter the current level 2 password when prompted.
4. Enter the new level 2 and level 1 PDT passwords when prompted. PDT passwords are case sensitive, must be 6 to 16 characters long, and the level 1 and 2 passwords must be different.

   To accept a password without changing it, press the <enter> key when prompted to enter a new password.
5. Exit PDT.
6. Verify the passwords by entering PDT with the current passwords.

Resetting the Passwords

On the large system, an install disk must be placed in the floppy drive. The On a 68000 series system, either drive can be used. On a CP PII system, only the drive on the active side can be used.

For Option 11C, the faceplate dip switch is used. Turn on the switch that corresponds to the next baud rate lower than it is currently set to and do not turn off the current switch. The two switches directly beside each other on the faceplate will be on.

Ensure that only two switches are on at any one time. Having three switches or more will cause an invalid condition and it will not be possible to communicate with the switch

After the disk is inserted, or the dip switch is turned on, use the following procedure to reset the password.

Procedure 2
Reset the password

1. Enter PDT using the site id as the password. For Option 11C, use the security id as the password.
2. At the PDT prompt, type ***passwd***.

3. When prompted for the current level 2 password, enter the tape id. For Option 11C, enter the security id. PDT passwords are case sensitive, must be 6 to 16 characters long, and the level 1 and 2 passwords must be different.

   To accept a password without changing it, press the <enter> key when prompted to enter a new password.

4. Enter the new level 2 and level 1 PDT passwords when prompted.

5. Remove the disk or power down the switch.

6. Exit PDT.

7. Verify the passwords by entering PDT with the current passwords.

Table 42
System Report messages for PDT (Part 1 of 3)

Report	Description / Action required	Severity
SRPT0051	PDT: PDT passwords set to default	Info
SRPT0052	PDT: Could not create PDT password file Try resetting the PDT passwords using the PASSWD command. If the PASSWD command fails or cannot be executed then: • For an Option 11C, enable the magic switch. Enter PDT using the systems SECURITY ID. Enter the PASSWD command and use the SECURITY ID as the Old PDT level 2 Password. • For all other systems, enter the install disk in the floppy drive of the active core. Enter PDT using the systems TAPE ID. Enter the PASSWD command and use the TAPE ID as the Old PDT level 2 Password. If this fails contact the system technical support group.	Minor
SRPT0053	PDT: Could not save PDT passwords Try resetting the PDT passwords using the PASSWD command. If the PASSWD command fails or cannot be executed then: • For an Option 11C, enable the magic switch. Enter PDT using the systems SECURITY ID. Enter the PASSWD command and use the SECURITY ID as the Old PDT level 2 Password. • For all other systems, enter the install disk in the floppy drive of the active core. Enter PDT using the systems TAPE ID. Enter the PASSWD command and use the TAPE ID as the Old PDT level 2 Password. If this fails contact the system technical support group.	Minor
SRPT0054	PDT: Passwords cannot be changed from a remote cabinet	Info
SRPT0055	PDT: Password changes have been stored	Info

Table 42
System Report messages for PDT (Part 2 of 3)

Report	Description / Action required	Severity
SRPT0056	PDT: Passwords can only be changed from the active side Check the core state using LD 135 stat CPU. Ensure the core is the active core. Try to change the passwords using the PASSWD command again. If this fails contact the system technical support group.	Info
SRPT0057	PDT: Problem detected with password synchronize • For an Option 11C: check the connection between the main cabinet and the remote cabinets. Ensure that the main cabinet and remote cabinets have completed their boot cycle. Try to change the passwords using the PASSWD command again. • For 68000 series systems, check that both cores are available, are synchronized and are joined. Try to change the passwords using the PASSWD command again. • For CP PII systems, check that the HSP is up, the systems are joined and the disks are synchronized. Try to change the passwords using the PASSWD command. If these actions fail, contact the system technical support group.	Minor
SRPT0058	PDT: Corrupt password detected Try resetting the PDT passwords using the PASSWD command. If the PASSWD command fails or cannot be executed then: • For an Option 11C enable the magic switch. Enter PDT using the systems SECURITY ID. Enter the PASSWD command and use the SECURITY ID as the Old PDT level 2 Password. • For all other systems, enter the install disk in the floppy drive of the active core. Enter PDT using the systems TAPE ID. Enter the PASSWD command and use the TAPE ID as the Old PDT level 2 Password. If these actions fail, contact the system technical support group.	Minor

Table 42
System Report messages for PDT (Part 3 of 3)

Report	Description / Action required	Severity
SRPT0059	PDT: Invalid password entered	Info
SRPT0060	PDT: Unexpected error occurred during PDT password changes Try to change the passwords using the PASSWD command. If the PASSWD command fails or cannot be executed then: • For an Option 11C enable the magic switch. Enter PDT using the systems SECURITY ID. Enter the PASSWD command and use the SECURITY ID as the Old PDT level 2 Password. • For all other systems, enter the install disk in the floppy drive of the active core. Enter PDT using the systems TAPE ID. Enter the PASSWD command and use the TAPE ID as the Old PDT level 2 Password. If these actions fail, contact the system technical support group.	Minor

Controlling access to system Application Processors

Restrict access to Application Processors by requiring a user to enter a valid user ID and password on the Application Processor console. The user can then access and run applications, or configure operating characteristics of the Application Processor.

System access privileges are based on user IDs that are password protected. Application Processors are Unix System V based self-contained modules that interface with the system. They can also interface to local and remote peripheral devices such as terminals, personal computers, and printers. Access is restricted by the user ID, not by the terminal. A user can log on with a user ID from any terminal, including the system console.

These UNIX-based Application Processors use a hierarchy of four basic user identifications, where number 1 is the highest and number 4 is the lowest. These user IDs are as follows:

- **root**
  First-level user ID used by authorized engineering and development personnel only. The **root** user ID is set during the application installation and is chosen based on the ID of the system to which it is connected. The **root** ID is different for each application.

- **disttech**
  Second-level user ID used by qualified field technicians, emergency technical assistance and service, and distributors to configure the Application Processor according to the customer applications requirements. This is also the second-level default password. The administrator must change this password when the system is first placed in service.

- **maint** or **mlusr**
  Third-level user IDs used by the customer application and maintenance administrator to install, modify, and remove applications running on the Application Processor. These are also the third-level default passwords.

- **mlusr** and **ccrusr**
  Application access user IDs and fourth-level user IDs used by the application user to access the Application Processor console, local or remote terminals, and personal computers to run applications. These are also the fourth-level default passwords. **ccrusr** is present only if CCR is installed**.**

To protect the Application Processor facilities from unauthorized access, adopt the following password management practices:

- avoid simple passwords or those that are derived from personal information such as social security number, home telephone number, birth dates, and so on.
- change passwords every 60 to 90 days.
- Change a password several times (a minimum of five) before a previously used password can be repeated.

- Use passwords at least eight characters in length and make them alphanumeric.
- The password must be changed at system cutover.
- Change the password immediately when anyone knowing the password leaves the company.

New system security planning

Contents

This section contains information on the following topics:

Introduction. 108

Analyzing the system configuration. 109

Filling out the security installation checklist. 109

System checklist. 110

Basic Access Restrictions. 110

Class of Service (CLS)). 110

Trunk Group Access Restrictions (TARG/TGAR). 111

Modifying Basic Access Restrictions. 111

System Speed Call (SSC) 111

Network Speed Call (NSC)) 112

Authorization Code (Authcode) 112

Forced Charge Account (FCA). 112

Enhanced and Controlled Class of Service (ECCS/CCOS) 113

Electronic Lock (ELK) 113

Code Restriction Blocks (CRB). 113

New Flexible Code Restriction (NFCR). 114

Called Party Disconnect Control (CPDC) 114

Call Forward (CFW). 114

User Selectable Call Redirection (USCR). 114

Call Forward External (CFXA/D) 115

Internal Call Forward (ICF) 115

Call Forward All Calls (CFW). 115

Call Forward to Trunk Access Code (CFTA). 116

Remote Call Forward (RCFW) 116

Call Forward Originating (CFO) or Forwarded (CFF) Class of Service 116
Basic/Network Automatic Route Selection 117
Supplemental Digit Recognition/Restriction (SDRR). 117
Network Class of Service (NCOS) and Facility Restriction Level (FRL). 117
Authorization Code Conditionally Last Network Authorization Code (NAUT) 118
Time of Day Schedule (TODS) 119
Routing Control (RTCL). 119
Incoming Trunk Group Exclusion (ITGE). 119
Free Calling Area Screening (FCAS) 120
TGAR Control (TGAR). 120
Direct Inward System Access (DISA) 121
Multi-Tenant (TENS) 121
SDI ports. 122
Call Detail Recording (CDR). 122
Traffic Reporting (TFC). 123
Meridian Mail checklist. 123
Call Answering/Express Messaging Thru-dial Restriction/Permission Code Tables. 123
Custom Voice Menu/Thru-dial Restriction/Permission Code Tables 124
Mailbox Password Assignment. 125
Password Parameters. 125

Introduction

This chapter describes how to evaluate new hardware and software security options for a new system using system software and Meridian Mail software. To plan security for a new system, do the following:

- Analyze the current system configuration
- Compare the current configuration to the new system
- Fill out the security installation checklist
- Evaluate the new hardware with the software security option

Analyzing the system configuration

When a new system is installed, security features necessary to protect call processing and administrative functions from unauthorized access must be activated.

It is easier for users to learn system security procedures once than to adjust to frequent changes later on. Making changes that affect the day-to-day operation of a company's PBX is disruptive to users and incoming callers alike.

Before installing security features, it is necessary to generate and install a configuration database. Based on this configuration, system security features can be designed to protect the system's call processing, administration, and maintenance functions.

To help define security for functions and features activated in the configuration database, use the security installation checklist. Refer to Appendix A in this document for a list of security features available.

Filling out the security installation checklist

The security installation checklist is designed to help provide the maximum protection for the system and its users. There is one checklist for the system and one for Meridian Mail.

This checklist is used by the customer and the distributor during the system configuration planning stage. For each function and feature in the customer configuration database, an equivalent security feature must be specified using the checklist. It can also be used when installation is complete to verify that all planned security features have been implemented. To verify these features, use the print program listed for each feature in this checklist.

The checklist is organized by feature. Each feature is divided into:

- **Print program –** The name of the program used to print data about the feature.
- **Guidelines –** Instructions on filling out security feature parameters.

- **Parameter values –** Security feature parameter values.
- The chapter and section to go to or the program to use to implement any proposed values.

To fill out each feature in the checklist, do the following:

1. Fill in the security feature parameter values.
2. Refer to the Implementation information for each security feature to implement the parameter values.

Before filling out the checklist, read "System security features" on page 17, and "System access security features" on page 87 to understand the system and Meridian Mail security features.

System checklist

Define all entries on the checklist that are configured in the system database. Skip entries that are not active in the system.

Basic Access Restrictions

Class of Service (CLS)

Print program – Terminal Number Block Program LD 20

Guidelines – Eight CLS Levels are available: UNR, CTD, CUN, TLD, SRE, FRE, FR1, and FR2. Specify one or more Levels for each item.

Single line/multi-line telephones	
DISA	
Authcodes	
TIE Trunks	
Meridian Mail Agents	

See "Class of Service" on page 20.

Trunk Group Access Restrictions (TARG/TGAR)

Print program – Terminal Number Block Program LD 20

Guidelines Specify a TARG/TGAR from 0 to 31 for each item, where 0 indicates no restrictions.

Single line/multi-line telephones _____
DISA _____
Authcodes _____
Meridian Mail Agents _____
Trunks _____
- COTS (TARG) _____
- WATS (TARG) _____
- DID (TARG) _____
- FEX (TARG) _____
- TIE (TARG on route) _____
- TIE (TGAR on individual trunks) _____
- PAG (TARG) _____
- MUS (TARG) _____

See “Trunk Group Access Restrictions” on page 23

Modifying Basic Access Restrictions

1. System Speed Call (SSC)

Print program – Speed Call List Program LD 20.

Guidelines – Specify an NCOS from 0 to 99 for the SSC list.

NCOS _____

See "System Speed Call" on page 26.

2. Network Speed Call (NSC)

Print program – Speed Call List Program LD 20

Guidelines – Enter the NSC list number to be used for specified long distance access.

NSC list number _____

See "Network Speed Call" on page 27.

3. Authorization Code (Authcode)

Print program – Authcode Data Block Program LD 88

Guidelines – Specify a CLAS from 1 to 115, a COS restriction Level of UNR, CTD, CUN, TLD, SRE, FRE, FR1, or FR2, a TGAR from 0 to 31, and an NCOS restriction Level from 0 to 99 for each Authcode in the system.

Authcode length _____ (4 to 16 digits)

CLAS _____ COS _____ TGAR _____ NCOS _____

CLAS _____ COS _____ TGAR _____ NCOS _____

CLAS _____ COS _____ TGAR _____ NCOS _____

CLAS _____ COS _____ TGAR _____ NCOS _____

CLAS _____ COS _____ TGAR _____ NCOS _____

CLAS _____ COS _____ TGAR _____ NCOS _____

See "Authorization Code" on page 28.

4. Forced Charge Account (FCA)

Print program – Customer Data Block Program LD 21

Guidelines – Select Yes to temporarily override toll-denied CLS restrictions. If Yes is selected, enter the length of the FCA.

FCC: Yes No (circle one)

FCC length _____ (4 to 5 digits)

See **Implementation** "Forced Charge Account" on page 32.

5. Enhanced and Controlled Class of Service (ECCS/CCOS)

Print program – Customer Data Block Program LD 21

Guidelines – Three different Levels are available. Identify the class of service for the three parameters, CCRS with either ECC1 and/or ECC2, or just ECC1, ECC2, or CCRS alone.

CCRS _____ ECC1 _____ ECC2 _____

See "Controlled Class of Service" on page 32 and "Enhanced Controlled Class of Service" on page 33.

6. Electronic Lock (ELK)

Print program – Customer Data Block Program LD 21

Guidelines – Select Yes to allow users to activate and deactivate CCOS mode from their telephones by entering the Station Control Password (SCPW) and the appropriate ELK code. If Yes is selected, enter the length of the SCPW.

ELK: Yes No (circle one)

SCPW length _____ (1 to 8 digits)

See "Electronic Lock" on page 34.

7. Code Restriction Blocks (CRB)

Print program – Route Data Program LD 21

Guidelines – Select Yes to allow toll-denied telephones and TIE trunks limited access to the toll exchange network over CO and FX trunks.

CRB: Yes No (circle one)

ALOW _____ DENY _____

See "Code Restriction Data Block" on page 35.

8. New Flexible Code Restriction (NFCR)

Print program – Customer Data Block Program LD 21

Guidelines – Select Yes to allow toll-denied telephones, TIE trunks, and Authcodes to selectively make certain calls on outgoing trunk routes.

NFCR: Yes No (circle one)

See "New Flexible Code Restriction" on page 36.

9. Called Party Disconnect Control (CPDC)

Print program – Route Data Program LD 21

Guidelines – Specify routes from 0 to 127 or check No if trunk-to-trunk transfers will not be prevented.

Route _____ _____ _____ _____ _____

No _____

See "Called Party Disconnect Control" on page 36.

Call Forward (CFW)

1. User Selectable Call Redirection (USCR)

Print program Terminal Number Block Program LD 20 and Station Administration Program LD 10/11

Guidelines Select USCR to restrict call forward destinations to external telephones.

IUSR Yes No (circle one)

SCPW length_____ (0 to 8 digits)

USR, FFC, SPCL (circle one or more)

See "User Selectable Call Redirection" on page 57.

2. Call Forward External (CFXA/D)

Print program Customer Data Block Program LD 21

Guidelines Select CFXD to restrict call forward from a telephone to an external DN.

CFXA CFXD (circle one)

See "Call Forward External Deny" on page 57.

3. Internal Call Forward (ICF)

Print program – Customer Data Block Program LD 21

Guidelines – Select ICF to allow user to route internal calls to a different location other than external calls.

ICF Yes No (circle one)
ICF length _____ 4 to 23 digits

See "Internal Call Forward" on page 58.

4. Call Forward All Calls (CFW)

Print program – Terminal Number Block Program LD 20 and Features and Station Print LD 81

Guidelines – Select CFW to allow call forward from a telephone to another location (internal or external).

CFW Yes No (circle one)
CFW length _____ (4 to 23 digits)

See "Call Forward All Calls" on page 59.

5. Call Forward to Trunk Access Code (CFTA)

Print program – Customer Data Block Program LD 21

Guidelines – Select No to restrict DID calls from being forwarded to a Trunk Access Code.

Trunk access code length _____ (1 to 4 digits – 7 with DN expansion)

CFTA: Yes No (circle one)

See "Call Forward to Trunk Access Code" on page 59.

6. Remote Call Forward (RCFW)

Print program – Customer Data Block Program LD 21

Guidelines – Select Yes to allow users to activate or deactivate call forwarding from remote telephones.

RCFW: Yes No (circle one)
RCFW Flexible Feature Code _____

See "Remote Call Forward" on page 61.

7. Call Forward Originating (CFO) or Forwarded (CFF) Class of Service

Print program – Customer Data Block Program LD 21

Guidelines – Select CFO or CFF to use CLS access privileges of the telephone that originates the call or the telephone that forwards the call.

CFF CFO (circle one)

See "Call Forward Originating or Forwarded Class of Service" on page 60.

Basic/Network Automatic Route Selection

1. Supplemental Digit Recognition/Restriction (SDRR)

Print program – ESN Data Block Program LD 86

Guidelines – Select Yes or No to allow or deny access to specific number sequences following NPAs, NXXs, or SPNs.

SDRR blocking 976 and 976 look alikes: Yes No (circle one)

SDRR blocking International "976-type" numbers: Yes No (circle one)

SDRR blocking 800/900 numbers: Yes No (circle one)

See "Supplemental Digit Recognition/Restriction" on page 62.

2. Network Class of Service (NCOS) and Facility Restriction Level (FRL)

Print program – Customer Data Block Program LD 21

Guidelines – Specify an NCOS from 0 to 99, a corresponding FRL from 0 to 7, and the calling area they are allowed to access, which can be area codes, geographic locations, exchanges, or special numbers.

NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____
NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____
NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____
NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____
NCOS	_____	NCOS	_____
FRL	_____	FRL	_____
Calling area	_____	Calling area	_____

See "Network Class of Service and Facility Restriction Level" on page 63.

3. Authorization Code Conditionally Last Network Authorization Code (NAUT)

Print program – Authcode Data Block Program LD 88.

Guidelines – Select Yes to prompt users who fail to meet the minimum FRL requirement assigned to a route to enter an Authcode to complete a call.

NAUT: Yes No (circle one)

See "Authorization Code Conditionally Last Network Authorization Codes" on page 64.

4. Time of Day Schedule (TODS)

Print program – Route List Index Program LD 86

Guidelines – There are eight time spans when routes are available for call processing. Each span is three hours long, from 12:00 a.m. and ending at 11:59 p.m. Check the time spans covered by BARS/NARS.

0 _____ 1 _____ 2 _____ 3 _____

4 _____ 5 _____ 6 _____ 7 _____

See "Time-of-Day Routing" on page 65.

5. Routing Control (RTCL)

Print program – Route Data Program LD 21

Guidelines – Circle Yes to reduce NCOS to lower Levels when the attendant console is in night mode or when the attendant activates the key that controls routing. If Yes for RTCL was circled, specify NMAP by entering the current NCOS and the NCOS value when the ETOD schedule is in effect. Enter a value of 1 to 7 for ETOD to specify the days of the week when RTCL is in effect, where 1 is Sunday and 7 is Saturday. One or more ETOD can be entered.

RTCL: Yes No (circle one)

NMAP _____ ETOD _____

See "Routing Control" on page 66.

6. Incoming Trunk Group Exclusion (ITGE)

Print program – ITGE Index Program LD 86

Guidelines – Specify routes from 0 to 511 and the area codes to be blocked on these routes.

Route _____ Block _____

Route _____ Block _____

Route _____ Block _____

Route _____ Block _____

Route _____ Block _____

Route _____ Block _____

See "Incoming Trunk Group Exclusion" on page 67.

7. Free Calling Area Screening (FCAS)

Print program – Route List Index Program LD 86

Guidelines – For each Route List Index (RLI), specify a number from 0 to 999 to define the Free Calling Index (FCI) 1 to 255 for each RLI entry. Specify 0 for the FCI if FCAS is not required.

Route List _____

Route List Entry _____ FCI _____

Route List Entry _____ FCI _____

Route List Entry _____ FCI _____

Route List Entry _____ FCI _____

Route List Entry _____ FCI _____

Route List Entry _____ FCI _____

See "Free Calling Area Screening" on page 68

8. TGAR Control (TGAR)

Print program – ESN Data Block Program LD 86

Guidelines – Select Yes to add TGAR access privileges to BARS/NARS as a qualification for call completion.

BARS/NARS TGAR: Yes No (circle one)

See "Trunk Group Access Restrictions" on page 23.

Direct Inward System Access (DISA)

Print program – Print DISA Block Program LD 24

Guidelines – Select the following parameters to define public access into the PBX for placing long distance calls over PBX facilities.

SCOD: Yes No (circle one) Length_____
Authcodes: Yes No (circle one) Length_____

DISA DN TGAR _____ CLS _____ NCOS _____

See "Controlling Direct Inward System Access" on page 69

Multi-Tenant (TENS)

Print program – Define Multi-Tenant Program LD 93

Guidelines – Specify a tenant from 1 to 511, a route from 0 to 999, and a Console Presentation Group (CPG) from 1 to 63.

Tenant-to-Tenant Access (TACC): Yes No (circle one)

Tenant _____ to Tenant _____

Tenant _____ to Tenant _____

Tenant _____ to Tenant _____

Tenant _____ to Tenant _____

Tenant _____ to Tenant _____

Tenant-to-Route Access (RACC): Yes No (circle one)

Tenant _____ to Route _____

Tenant _____ to Route _____

Tenant _____ to Route _____

Tenant _____ to Route _____

Tenant _____ to Route _____

Console Presentation Groups (CPG): Yes No (circle one)

CPG _____ for Tenants _____

CPG _____ for Tenants _____

CPG _____ for Tenants _____

CPG _____ for Tenants _____

CPG _____ for Tenants _____

See "Controlling Multi-Tenant Services" on page 71.

SDI ports

1. Call Detail Recording (CDR)

Print program – Configuration Record Program LD 22

Guidelines – Specify the CDR port that connects the CDR terminal to the system and enter routes programmed to output CDR from 0 to 999 and if there are incoming, outgoing, two way, and so on.

CDR Port number _____

Route _____ Type _____ Route _____ Type _____

Route _____ Type _____ Route _____ Type _____

Route _____ Type _____ Route _____ Type _____

See "Analyzing Call Detail Recording reports" on page 178.

Traffic Reporting (TFC)

Print program – Configuration Record Program LD 22.

Guidelines – Specify the port that connects the traffic terminal to the system and specify traffic parameters required to collect and report traffic statistics.

Traffic	Port number _____
Schedule	_____
Which reports are scheduled	_____
Traffic Log	Yes No (circle one)

See "Analyzing Traffic Measurement reports" on page 182.

Meridian Mail checklist

Define all entries in the checklist that are configured for Meridian Mail. Skip entries that are not active. Note the reason why the feature is not active.

1. Call Answering/Express Messaging Thru-dial Restriction/Permission Code Tables

Print program – Voice Security Option screen

Guidelines – Specify 1- to 5-digit extension numbers, trunk access codes, special prefix codes, or BARS/NARS access codes that callers are permitted to use, or restricted from using. Ten permission and ten restriction codes are allowed for each table. Name defaults are On-Switch, Local, Long Distance 1, or Long Distance 2. Users can select their own table names.

Name	_____				
Restrict	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____
Permit	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____
Name	_____				
Restrict	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____
Permit	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____

Name _____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Name _____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

See “Controlling Voice Menu/Thru-dialer” on page 79

2. Custom Voice Menu/Thru-dial Restriction/Permission Code Tables

Print program – Voice Menu Thru Dialers

Guidelines – Specify 1- to 5-digit extension numbers or area codes that callers are permitted to use or restricted from using. Ten permission and ten restriction codes are allowed for each table.

Menu Name _____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Menu Name _____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Menu Name _____

Restrict _____ _____ _____ _____ _____

_____ _____ _____ _____ _____

Permit _____ _____ _____ _____ _____

	_____	_____	_____	_____	_____
Menu Name	_____				
Restrict	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____
Permit	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____

See “Controlling Voice Menu/Thru-dialer” on page 79.

3. Mailbox Password Assignment

Print program – Voice Security Option screen

Guidelines – Specify if the mailbox password is to be a default or an administrator assigned password.

Default _____ Administrator Assigned _____ (check one)

Password prefix Yes No (circle one)

See “Controlling Voice Menu/Thru-dialer” on page 79.

4. Password Parameters

Print program – Voice Security Option screen

Guidelines Used to limit unauthorized access to voice mail.

Invalid log-in attempts per session	_____
Invalid log-in attempts per mailbox	_____
Minimum password length	_____
Forced password change	_____
Number of days between changes	_____
Number of changes before password repeats	_____
Expiration warning	Yes No (circle one)
Expiration warning schedule	_____

Existing system security upgrade

Contents

This section contains information on the following topics:

Introduction. . ... .128

Auditing system security features 129

System audit checklist 129

Audit Trail 130
Authorization Code (Authcode) 130
Background Terminal 131
Call Detail Recording..... 131
Call Forward to Trunk Access Codes (CFTA).....132
Call Forwarding: Forwarding (CFF) or Originating (CFO) Control..132
Central Office Translation (NXX) 133
Code Restriction (CRB).....133
Console Presentation Group (CPG).....134
Controlled Class of Service (CCOS) 135
Coordinated Dialing Plan (CDP).....135
Customer Night Numbers.....136
Digit Manipulation Index (DGT) 136
Direct Inward System Access (DISA) 137
ESN Data Block (ESN) 137
Flexible Feature Code (FFC).....138
Forced Charge Account (FCA) 139
History File 140
Incoming Trunk Group Exclusion (ITGE) 140
Location Code (LOC) 141
Meridian Mail – Virtual Agent data.....141
Multi-line telephones 142
Network Control (NTCL)..... 143

Network Speed Call (NSC)..... 144
New Flexible Code Restriction (NFCR)..... 144
Numbering Plan Area Code (NPA)..... 145
Passwords 146
Route List Index (RLI)..... 147
Secure Data Password (SPWD).....148
Single-line telephones..... 149
Special Number Translation (SPN).....150
System Speed Call (SSC) 151
Telephone Control Password Length..... 151
Tenant-to-Route Access (RACC) 152
Tenant-to-Tenant Access (TACC) 152
Traffic Log..... 153
Traffic Terminal.....153
Trunk Route and CDR control 153
Trunks 155
Auditing Meridian Mail security features. 157
Meridian Mail audit checklist. 157
Call Answering/Express Message Outcalling Thru-dial 157
Directory Number Table.....160
Express Messaging Thru-dial..... 160
Passwords..... 161
Password parameters..... 161
Thru-dial..... 162
Voice Menu Thru-dial..... 162
Auditing Application Processor security features. 163

Introduction

This chapter describes how to plan an existing system security upgrade. It describes security audit procedures used to analyze existing system security and define additional security features as required. The following security features are audited:

- system security features
- Meridian Mail security features
- system Application Processor security features

Note: Auditing an existing system assumes an in-depth working knowledge of system software including prompts and responses. Users must contact their Nortel Networks distributor for assistance in conducting this audit if they are not trained and certified in system software and/or Meridian Mail software.

Before filling out the checklist, read "System security features" on page 17, "Meridian Mail security features" on page 75, and "System access security features" on page 87 to understand the system and Meridian Mail security features.

Auditing system security features

System security includes call processing security features, system administration, and maintenance security features. To audit existing security, use the system audit checklist. Refer to Appendix A in this manual for a list of security features available

System audit checklist

The checklist is organized by feature. Each feature is divided into:

- **Print program** – The name of the program used to print data about the feature.
- **Guidelines** – Instructions on filling out proposed values.
- **Parameter values** – Current feature values and proposed feature values.
- The chapter and section to review or the program to use to implement any proposed values.

To fill out each feature in the checklist, do the following:

1. Print out data about the feature using the **Print program** information.
2. Fill in the **Current values** column using the information generated by the **Print program**.

3 Use the **Guidelines** to fill out the **Proposed value** column. If retaining the current value, enter a check mark in this column.

4 Refer to the **Implementation** information to change current values to **Proposed values**.

1. Audit Trail

Print program – Audit Trail Program LD 22. Only the administrator with a Level 2 password is allowed to print the contents of the Audit Trail.

Guidelines – Determine if an Audit File exists. If there is no file, activate one. Ensure that the file is large enough to hold all possible entries. Increase the size if necessary. To allow manual initialization of a port locked out due to invalid log-on attempts, set INIT = Yes.

Parameter	Current value	Proposed value
AUDT	Yes No (circle one)	Yes No (circle one)
SIZE	_____	_____
INIT	Yes No (circle one)	Yes No (circle one)

See "Audit Trail review" on page 93.

2. Authorization Code (Authcode)

Print program – Authcode Data Block Program LD 88

Guidelines – Ensure that CDR is recording the Authcodes. Determine the COS, TGAR, and NCOS for each CLAS. There must be no duplicate CLASs.

Parameter	Current value	Proposed value
SPWD	_____	_____
ALEN	_____	_____
ACDR	_____	_____
CLAS	_____	_____
COS	_____	_____
TGAR	_____	_____
NCOS	_____	_____

Verify the following for each Authcode:

Parameter	Current value	Proposed value
SPWD	_____	_____
CODE	_____	_____
CLAS	_____	_____

See "Authorization Code" on page 71.

3. Background Terminal

Print program – Configuration Record Program LD 22

Guidelines – Identify if a Background Terminal exists and is used for Controlled Class of Service.

Parameter	Current value	Proposed value
ADAN	TTY_____	TTY_____
USER	BGD	BGD
CUST	_____	_____
MANU	_____	_____

See Configuration Record Program LD 17.

4. Call Detail Recording

Print program – Configuration Record Program LD 22

Guidelines – Identify which port is assigned CDR output. Check to ensure activity. If there is no CDR, disregard all other references to CDR.

Parameter	Current value	Proposed value
ADAN	TTY_____	TTY_____
USER	CTY	CTY
CDR port assigned	_____	_____
CDPR	Yes No (circle one)	Yes No (circle one)
CLID	Yes No (circle one)	Yes No (circle one)

See "Analyzing Call Detail Recording reports" on page 178.

5. Call Forward to Trunk Access Codes (CFTA)

Print program – Customer Data Block Program LD 21

Guidelines – This prompt must be set to No. If forwarding to Trunk Access Codes is allowed, users can forward incoming calls to outbound trunks. If the telephone's TGAR does not allow direct access, this feature is not active even if allowed.

Parameter	Current value	Proposed value
CFTA	Yes No (circle one)	Yes No (circle one)

See "Call Forward to Trunk Access Code" on page 59.

6. Call Forwarding: Forwarding (CFF) or Originating (CFO) Control

Print program – Customer Data Block Program LD 21

Guidelines – Note if OPT = CFF or CFO. CFO indicates that the originator of the call has the controlling CLS when the called telephone is in Call Forward All Calls. If OPT = CFO, check the CLS, TGAR, and NCOS of the DID trunk and Route Data Blocks. DID trunks must be restricted from external calling or long distance calling through BARS/NARS and denied direct access to other trunk groups. The option CFF indicates that the telephone being called carries the controlling CLS for call processing in Call Forward All Calls.

Current value	Proposed value
OPT = CFF or CFO (Circle one)	OPT = CFF or CFO (Circle one)
If CFO, CLS, TGAR and NCOS on DID trunks =_____	If CFO, CLS, TGAR and NCOS on DID trunks =_____

See "Controlling Call Forward access" on page 56.

7. Central Office Translation (NXX)

Print program – Central Office Translation Program LD 90

Guidelines – Eliminate NXX 976 if programmed. Highlight any numbers with inconsistent routing and/or digit manipulation.

Parameter	Current value	Proposed value
TRAN	_____	_____
NXX	_____	_____
RLI	_____	_____
SDRR	_____	_____
DMI	_____	_____
DENY	_____	_____
LDID	_____	_____
LDDD	_____	_____
DID	_____	_____
DDD	_____	_____
ITED	_____	_____
ITEI	_____	_____

See Central Office Translation Program LD 90. New NXX configuration parameters will be in effect when implementing NXX-related security features in “Supplemental Digit Recognition/Restriction” on page 62 and “Incoming Trunk Group Exclusion” on page 67.

8. Code Restriction (CRB)

Print program – Code Restriction Data Program LD 21

Guidelines – Review the ALOW and DENY entries for each CRB on each route. Indicate those that permit long distance dialing and have no BARS/NARS access to control call routing.

Parameter	Current value	Proposed value
ROUT	_____	_____
CLR	ALOW or DENY	ALOW or DENY
ALOW or DENY	_____	_____

If the system is required to permit equal access capability, verify that only operator assisted or credit card calls are accessible. Allowing direct dialed equal access capabilities affects all telephones, DISA DNs, Authcodes, TIE trunks, and voice mail virtual agent ports.

Identify all programming for Feature Group D:

Parameter	Current value	Proposed value
FGNO	_____	_____
LDAC	AC1 or AC2	AC1 or AC2
LAAC	AC1 or AC2	AC1 or AC2
OPER	_____	_____
INIT	_____	_____

See “Code Restriction Data Block” on page 35.

9. Console Presentation Group (CPG)

Print program – Multi-Tenant Service Program LD 93

Guidelines – Indicate if any night numbers for any CPGs are Meridian Mail DNs.

Parameter	Current value	Proposed value
CPG	_____	_____
NIT1	_____	_____
NIT2	_____	_____
NIT3	_____	_____
NIT4	_____	_____

See “Controlling Multi-Tenant Services” on page 71.

10. Controlled Class of Service (CCOS)

Print program – Customer Data Block Program LD 21

Guidelines – Identify the three (maximum) CLS assignments.

Parameter	Current value	Proposed value
CCRS (Rel. 7 or later)	_____	_____
ECC1 (Rel. 15 or later)	_____	_____
ECC2 (Rel. 15 or later)	_____	_____

See "Controlled Class of Service" on page 32 and "Enhanced Controlled Class of Service" on page 33.

11. Coordinated Dialing Plan (CDP)

Print program – Coordinated Dialing Plan Program LD 87

Guidelines – Provide the following information for each Distant Steering Code (DSC), Local Steering Code (LSC), and Trunk Steering Code (TSC).

Parameter	Current value	Proposed value
LSC, DSC, or TSC	_____	_____
DEL (LSC)	_____	_____
RLI (DSC, TSC)	_____	_____

See Coordinated Dialing Plan Program LD 87. New CDP configuration parameters will be in effect when implementing CDP-related security features in "Supplemental Digit Recognition/Restriction" on page 62 and "Incoming Trunk Group Exclusion" on page 67.

12. Customer Night Numbers

Print program – Customer Data Block Program LD 21

Guidelines – Identify the night numbers and determine if any NITE DNs are Meridian Mail ACD-DNs. Indicate those that are Meridian Mail ACD-DNs by an "M" after the number.

Parameter	Current value	Proposed value
NITE	_____	_____
NIT1	_____	_____
TIM1	_____	_____
NIT2	_____	_____
TIM2	_____	_____
NIT3	_____	_____
TIM3	_____	_____
NIT4	_____	_____
TIM4	_____	_____

See Customer Data Block Program LD 15. These parameters will be in effect for customer-related security features.

13. Digit Manipulation Index (DGT)

Print program – Digit Manipulation Index Program LD 86

Guidelines – Note any DGTs that delete internal numbers and insert complete external numbers. Verify that these numbers are valid, especially if they are routed to another area code.

Parameter	Current value	Proposed value
DMI	_____	_____
DEL	_____	_____
INST	_____	_____

See Digit Manipulation Index Program LD 86. New DGT configuration parameters will be in effect when implementing DGT-related security features in "Supplemental Digit Recognition/Restriction" on page 62.

14. Direct Inward System Access (DISA)

Print program – Print DISA Block Program LD 24

Guidelines – If there are no DISA DNs active on the system, no plans to activate DISA, and the DISA software is resident on PKG, consider having DISA removed from the base software of the diskettes or tapes. Eliminate the possibility of database abuse whenever possible.

Determine if SCODs and Authcodes are required. DISA directory numbers must not directly access trunks by using access codes. DISA DNs requiring Authcodes must carry a low COS and NCOS. The Authcode is the mechanism that overrides the DISA directory number CLS.

Parameter	Current value	Proposed value
SPWD	_____	_____
DN	_____	_____
SCOD	_____	_____
AUTR	Yes No (circle one)	Yes No (circle one)
TGAR	_____	_____
NCOS	_____	_____
CLS	_____	_____

See “Controlling Direct Inward System Access” on page 69.

15. ESN Data Block (ESN)

Print program – ESN Data Block Program LD 86

Guidelines – Verify if the system uses CDP and how many digits are in a steering code. List codes for AC1 and AC2 and list time schedules for TODS. Indicate if RTCL is used and when it is effective. State if TGAR is used in addition to the standard BARS/NARS controls for access to trunk routes. TGAR control is commonly used in Multi-tenant environments.

Parameter	Current value	Proposed value
CDP	Yes No (circle one)	Yes No (circle one)
MXSC	_____	_____
NCDP	_____	_____
AC1	_____	_____
AC2	_____	_____
TODS	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____
RTCL	Yes No (circle one)	Yes No (circle one)
NMAP	_____	_____
ETOD	_____	_____
TGAR	Yes No (circle one)	Yes No (circle one)

See ESN Data Block Program LD 86. New ESN block configuration parameters will be in effect when implementing ESN-related security features in “Supplemental Digit Recognition/Restriction” on page 62, “Authorization Code Conditionally Last Network Authorization Codes” on page 64, “Time-of-Day Routing” on page 65, and “Incoming Trunk Group Exclusion” on page 67.

16. Flexible Feature Code (FFC)

Print program – Print FFC Data Program LD 57

Guidelines – These features allow activation of access features such as Call Forward, ELK, SSC, and SCPD change.

Parameter	Current value	Proposed value
ASRC	_____	_____
AUTH	_____	_____
CDRC	_____	_____
CFWA	_____	_____
CFWD	_____	_____
CFWV	_____	_____
DEAF	_____	_____
ELKA	_____	_____
ELKD	_____	_____
RCFA	_____	_____
RCFD	_____	_____
RCFV	_____	_____
SCPC	_____	_____
SSPU	_____	_____

See “Electronic Lock” on page 34.

17. Forced Charge Account (FCA)

Print program – Customer Data Block Program LD 21

Guidelines – If FCAF = Yes, identify the number length of the FCA, the minimum number of digits, and the NCOS for network FCA.

Parameter	Current value	Proposed value
CHLN	_____	_____
FCAF	Yes No (circle one)	Yes No (circle one)
CHMN	_____	_____
FCNC	_____	_____

See “Forced Charge Account” on page 32.

18. History File

Print program – History File Program LD 22

Guidelines – Verify that a History File exists. Make certain that the file is large enough to hold the activity directed to it. Review the type of messages being sent to the history file. Print the history file to verify the content. Eliminate outputting all unnecessary messages.

Parameter	Current value	Proposed value
HIST	_____	Rel. 17 and earlier
ADAN	HST	Rel. 18 and later
USER	_____	_____

See "History File review" on page 94.

19. Incoming Trunk Group Exclusion (ITGE)

Print program – Incoming Trunk Group Exclusion Index Program LD 86

Guidelines – Determine what numbers ITGEs are blocking. Decide if they are programmed effectively and test to ensure correct application.

Parameter	Current value	Proposed value
ITEI	_____	_____
RTNO	_____	_____

See Incoming Trunk Group Exclusion Index Program LD 86. New ITGE configuration parameters will be in effect when implementing ITGE-related security features in "Incoming Trunk Group Exclusion" on page 67.

20. Location Code (LOC)

Print program – Location Code Program LD 90

Guidelines – Determine DGT for each entry on the RLI. Indicate if DGT modifies calls to a specific external location. Validate location and telephone number.

Parameter	Current value	Proposed value
TRAN	_____	_____
LOC	_____	_____
RLI	_____	_____
ITEG	_____	_____
LDN	_____	_____
DID	Yes No (circle one)	Yes No (circle one)
MNXX	Yes No (circle one)	Yes No (circle one)
SAVE	_____	_____
OFFC	_____	_____
RNGE	_____	_____

See Location Code Program LD 90. New LOC configuration parameters will be in effect when implementing LOC-related security features.

21. Meridian Mail – Virtual Agent data

Print program – Terminal Number Block Program LD 11.

Guidelines – Identify the ACD-DNs associated with Meridian Mail. List the system software for each virtual agent position ID and review to ensure that each is the lowest NCOS, FRL, CLS possible and cannot directly access any outbound trunk route. Flag any exceptions.

Parameter	Current value	Proposed value
ACDN	_____	_____
Voice Mail DN	Yes No (circle one)	Yes No (circle one)
NCFW	_____	_____
Meridian Mail	Yes No (circle one)	Yes No (circle one)

Virtual Agent Position IDs and Associated CLS, NCOS, TGAR

Current value		**Proposed value**	
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

See ACD Directory Number Program LD 23.

22. Multi-line telephones

Print program – Terminal Number Blocks Program LD 20

Guidelines – Make note of all virtual ports that are used for access to a voice mail system. Ensure that they are as restricted as possible to prohibit calls from transferring out of the mail system to the PBX and making unauthorized toll calls.

Enter the TGAR definitions on the TGAR matrix. The matrix will show direct access capabilities of multi-line telephones. All multi-line telephones must be restricted from direct access of outbound facilities unless BARS/NARS is not programmed to process calls. If direct access is the only method of making outbound calls from multi-line telephones, review CRB and NFCR data blocks to ensure authorized access of facilities.

SCPW must be as long as possible; codes up to eight digits are allowed. Each SCPW must be unique.

Verify that Call Forward digits are no greater than necessary. If the system has 4-digit extensions, CFW4 is sufficient. All telephones must be programmed as CFXD. This prohibits call forwarding to access codes such as AC1 and AC2, Trunk Access Codes, and numbers external to the PBX. There should be very rare exceptions allowing external Call Forward.

UNR allows unrestricted calls. CTD is recommended. Use TLD, SRE, FRE, FR1, and FR2 whenever possible.

Indicate telephones that are assigned CCSA, SSU, FCA, and/or TENA. These features when active will affect access restrictions and controls.

For each multi-line telephone, identify the following:

Parameter	**Current value**	**Proposed value**
TGAR	_____	_____
NCOS	_____	_____
SSU	_____	_____
SCPW	_____	_____
CLS	_____	_____
(UNR - CFXA, CCSA, TENA, ICDA, AUTR, AUTU, AUTD)		
EFD	_____	_____
EHT	_____	_____
TEN	_____	_____
FCAR	Yes No (circle one)	Yes No (circle one)
KEY		
CFW (no. of digits)	_____	_____
CHG	_____	_____

See Multi-line Telephone Administration Program LD 11. These new telephone configuration parameters will be in effect when implementing multi-line telephone-related security features.

23. Network Control (NTCL)

Print program – Network Control Program LD 87

Guidelines – Each NCOS is defined to restrict calls to specific calling patterns. NCOSs are traditionally built with increasing call capabilities.

Lower numbered NCOSs are usually most restrictive and higher numbered NCOSs are least restrictive. One NCOS must not duplicate another. Print out the entire NCOS database to ensure that a rogue code is not built at the end of the database.

Parameter	Current value	Proposed value
NCOS	_____	_____
EQA	_____	_____
FRL	_____	_____
RWTA	Yes No (circle one)	Yes No (circle one)
NSC	Yes No (circle one)	Yes No (circle one)
LIST	Yes No (circle one)	Yes No (circle one)

See Network Control Program LD 87. New NTCL configuration parameters will be in effect when implementing NTCL-related security features in "New Flexible Code Restriction" on page 36, "Network Speed Call" on page 27, "Authorization Code Conditionally Last Network Authorization Codes" on page 64, and "Routing Control" on page 66.

24. Network Speed Call (NSC)

Print program – Network Translation Program LD 90

Guidelines – Select a BARS/NARS access code and specify a 1- to 3-digit Network Speed Call Access Code (NSCC) and a 0 to 4095 System Speed Call List (SSCL) number.

Parameter	Current value	Proposed value
TRAN	AC1 or AC2	AC1 or AC2
NSCC	_____	_____
SSCL	_____	_____

See "Network Speed Call" on page 27.

25. New Flexible Code Restriction (NFCR)

Print program – Print Data Program LD 49

Guidelines – Identify trees used for Feature Group D, all trees allowing long distance calls and operator assisted calls.

If selecting Yes for NFCR, specify MAXT from 1 to 255 to define the maximum number of NFCR trees.

If the system is required to permit equal access capability, verify that only operator assisted or credit card calls are accessible. Allowing direct dialed equal access capabilities affects all telephones, DISA DNs, Authcodes, TIE trunks, and voice mail virtual agent ports.

Verify if the Central Office provides a service that prohibits bill back to the telephone placing an equal access call. This will prohibit callers dialing 010XXX from using the listed directory number or DN as a bill number instead of a credit card number.

Parameter	**Current value**	**Proposed value**
NFCR	Yes No (circle one)	Yes No (circle one)
MAXT	_____	_____
CRNO	_____	_____
ALOW and/or DENY	_____	_____
BYPS	_____	_____

See "New Flexible Code Restriction" on page 36.

26. Numbering Plan Area Code (NPA)

Print program – Numbering Plan Area Code Program LD 90

Guidelines – Indicate area codes to international locations and if they are sent to a route different from U.S. long distance calling. The route must be different to indicate special status; it must carry a higher NCOS and have an FCAS table to permit calling to specific business numbers within a high-fraud

area code such as 809. If a company doesn't call the 809 area, remove it from the translation tables.

Parameter	Current value	Proposed value
TRAN	_____	_____
NPA	_____	_____
RLI	_____	_____
SDRR	_____	_____
DMI	_____	_____
DENY	_____	_____
LDID	_____	_____
LDDD	_____	_____
DID	_____	_____
DDD	_____	_____
ITED	_____	_____
ITEI	_____	_____

See Numbering Plan Area Code Program LD 90. New NPA configuration parameters will be in effect when implementing NPA-related security features in "Supplemental Digit Recognition/Restriction" on page 62, "Incoming Trunk Group Exclusion" on page 67, and "Free Calling Area Screening" on page 68.

27. Passwords

Print program – Passwords Program LD 22

Guidelines – Verify all passwords. Ensure that all passwords have been changed from the default value. Passwords must be a maximum of eight characters in length. Make all passwords complex alphanumeric entries and nonrepetitive. Change all passwords that are obvious.

Limit access to administration and maintenance programs (overlays) by allowing a specific password to access only selected programs and restricting access to all other programs. Where necessary, allow users to change their own passwords.

Parameter	**Current value**	**Proposed value**
LAPW	_____	_____
PWnn	_____	_____
LOGIN_NAME	_____	_____
OVLA	_____	_____
CUST	_____	_____
TEN	_____	_____
HOST	Yes No (circle one)	Yes No (circle one)
OPT (Circle A or D):		
	CFPD (A)	CFPD (A)
	LLCA (D)	LLCA (D)
	PROA (D)	PROA (D)
	PSCD (A)	PSCD (A)
LPWD	_____	_____
FLTH	_____	_____
LOCK	_____	_____
Multi-User	_____	_____

See “Program access control” on page 92.

28. Route List Index (RLI)

Print program – Route List Index Program LD 86

Guidelines – Note any RLIs that deviate from consistent programming: no TODs, DGTs to external numbers, low FRLs, FCAS tables for long distance routing, or unusual route patterns. Make note of which NPAs, NXXs, SPNs, DSCs, TSCs, or LOCs are routed to these RLIs.

Parameter	Current value	Proposed value
RLI	_____	_____
ENTR	_____	_____
ROUT	_____	_____
TOD	_____	_____
CNV	Yes No (circle one)	Yes No (circle one)
EXP	Yes No (circle one)	Yes No (circle one)
FRL	_____	_____
DMI	_____	_____
FCI	_____	_____
MFRL	_____	_____

See Route List Index Program LD 86. New RLI configuration parameters will be in effect when implementing RLI-related security features in "Authorization Code Conditionally Last Network Authorization Codes" on page 64, "Time-of-Day Routing" on page 65, and "Free Calling Area Screening" on page 68.

29. Secure Data Password (SPWD)

Print program – Customer Data Block Program LD 21 to display passwords

Guidelines – Verify that a password exists to change Authcodes and DISA information. Activate a password when DISA and Authcodes are used.

Parameter	Current value	Proposed value
SPWD	_____	_____

See "Authorization Code" on page 71.

30. Single-line telephones

Print program – Terminal Number Block Program LD 20

Guidelines – Make note of all virtual ports that are used for access to a voice mail system. Ensure ports are as restricted as possible to prohibit calls from transferring out of the mail system to the PBX and making unauthorized toll calls.

Enter the TGAR definitions on the TGAR matrix. The matrix will show direct access capabilities of single line telephones. All single line telephones must be restricted from direct access of outbound facilities unless no BARS/NARS is programmed to process calls. If direct access is the only method of making outbound calls from single line telephones, review CRB and NFCR data blocks to ensure authorized access to facilities.

SCPWs must be as long as possible; codes up to eight digits are permissible. Each SCPW must be unique.

Verify that Call Forward digits are no greater than necessary. If the system has 4-digit extensions, CFW4 is sufficient. All telephones must be programmed as CFXD. This prohibits call forwarding to access codes such as AC1 and AC2, Trunk Access Codes, and numbers external to the PBX. There should be very rare exceptions allowing external Call Forward.

UNR CLS allows unrestricted calls. CTD is recommended. Use TLD, SRE, FRE, FR1, and FR2 whenever possible.

Identify all telephones that Hunt or Forward No Answer out of the system and their hunt or no answer location. Restrict this ability whenever possible.

Indicate telephones that are assigned CCSA, SSU, FCA, and/or TENA. These features when active will indicate possible access restrictions and controls.

For each single line telephone, identify the following:

Parameter	Current value	Proposed value
TGAR	_____	_____
NCOS	_____	_____
SCPW	_____	_____
CLS	_____	_____
(UNR - CFXA, CCSA, TENA, ICDA, AUTR, AUTU, AUTD)		
TEN	_____	_____
FCAR	Yes No (circle one)	Yes No (circle one)
FTR		
CFW (no. of digits)	_____	_____
EHT	_____	_____
EFD	_____	_____
SSU	_____	_____

See Single-line Set Administration Program LD 10. These new telephone configuration parameters will be in effect when implementing telephone-related security features.

31. Special Number Translation (SPN)

Print program – Network Translation Program LD 90

Guidelines – Check for entries permitting equal access calls. Ensure these entries do not override entries in CRB or NFCR databases. Check for entries of country codes. If there is no international dialing, eliminate any entries for international dialing from the table. If international calls are permitted, define Levels to the country code if possible. Restrict using flexible ESN routing for 0, 00, 01, 011, and Supplemental Digit Recognition/Restriction (SDRR).

Parameter	Current value	Proposed value
TRAN	_____	_____
SPN	_____	_____
RLI	_____	_____
SDRR	_____	_____
DMI	_____	_____
DENY	_____	_____
LDID	_____	_____
LDDD	_____	_____
DID	_____	_____
DDD	_____	_____
ITED	_____	_____
ITEI	_____	_____

See Network Translation Program LD 90. New SPN configuration parameters will be in effect when implementing SPN-related security features in “Supplemental Digit Recognition/Restriction” on page 62 and “Incoming Trunk Group Exclusion” on page 67.

32. System Speed Call (SSC)

Print program – Speed Call List Program LD 20

Guidelines – Verify SSC lists and entries.

Parameter	Current value	Proposed value
LNSO	_____	_____
NCOS	_____	_____
STOR	_____	_____

See “System Speed Call” on page 26.

33. Telephone Control Password Length

Print program – Customer Data Block Program LD 21

Guidelines – Indicate the number of digits allowed for a telephone control password. The recommended minimum is six.

Parameter	Current value	Proposed value
SCPL	_____	_____

See "Electronic Lock" on page 34.

34. Tenant-to-Route Access (RACC)

Print program – Multi-Tenant Service Program LD 93

Guidelines – Identify any RACC restrictions.

Parameter	Current value	Proposed value
ROUT	_____	_____
ACC	ALOW or DENY	ALOW or DENY
DENY	_____	_____
ALOW	_____	_____

See "Controlling Multi-Tenant Services" on page 71.

35. Tenant-to-Tenant Access (TACC)

Print program – Multi-Tenant Service Program LD 93

Guidelines – Identify any TACC restrictions.

Parameter	Current value	Proposed value
TEN	_____	_____
ACC	ALOW or DENY	ALOW or DENY
DENY	_____	_____
ALOW	_____	_____

See "Controlling Multi-Tenant Services" on page 71.

36. Traffic Log

Print program – Configuration Record LD 22

Guidelines – Identify the size of the traffic log. Determine from Traffic LD2 when traffic reports are scheduled. Verify which reports are scheduled, when they are scheduled, and how often they are checked. If there is a third party device that captures and processes traffic information, identify the hardware and software.

Parameter	Current value	Proposed value
ADAN	TRF_____	TRF_____
SIZE	_____	_____

37. Traffic Terminal

Print program – Configuration Record Program LD 22

Guidelines – Identify the traffic terminal. Determine from Traffic Program LD 2 when traffic programs are scheduled. Verify which reports are scheduled and how often they are checked. If there is a third-party device that captures and processes traffic information, identify the hardware and software.

Parameter	Current value	Proposed value
ADAN	TTY_____	TTY_____
USER	TRF	TRF
CUST	_____	_____
Third-Party Device	_____	_____

See “Analyzing Traffic Measurement reports” on page 182.

38. Trunk Route and CDR control

Print program – Route Data Block Program LD 21

Guidelines – Highlight all AUTO routes. Label any routes that are DISA or auto-terminating to the automated attendant.

Verify that all routes configured as Incoming Trunks (ICT) or Outgoing Trunks (OGT) are sent one way from the CO. The caution here is that some trunks are two way from the CO and configured as one way at the PBX, inadvertently allowing access to or from the public network.

Routes configured as CPDC = Yes are unable to be transferred to another route for outbound traffic. This is a systemwide parameter and effective for any call using the route. There is no override.

Ensure that all routes carrying outbound traffic are configured to output CDR and identify the types of CDR they will output.

If the route uses NFCR, note the FRL and tree number.

Using the **TGAR worksheet** form, which is a TARG/TGAR matrix, enter the trunk type access code and TARG of each route as a horizontal entry. Refer to the TGAR worksheet form in Appendix Band use this form to configure the routes.

Parameter	**Current value**	**Proposed value**
ROUT	_____	_____
TKTP	_____	_____
PRIV	_____	_____
ISDN	_____	_____
AUTO	Yes No (circle one)	Yes No (circle one)
ICOG	_____	_____
ACOD	_____	_____
TARG	_____	_____
CPDC	Yes No (circle one)	Yes No (circle one)
CDR	Yes No (circle one)	Yes No (circle one)
INC	Yes No (circle one)	Yes No (circle one)
QREC	Yes No (circle one)	Yes No (circle one)
QAL	Yes No (circle one)	Yes No (circle one)
QTL	Yes No (circle one)	Yes No (circle one)
AIA	Yes No (circle one)	Yes No (circle one)
OAN	Yes No (circle one)	Yes No (circle one)
OPD	Yes No (circle one)	Yes No (circle one)

NATL	Yes No (circle one)	Yes No (circle one)
TDG	_____	_____
FRL	_____	_____

For trunks where TYPE = TIE, ISDN = YES, and ISAR = YES, record the following:

Parameter	**Current value**	**Proposed value**
NCOS	_____	_____
CLS	_____	_____
TGAR	_____	_____

See system security features Trunk Route and CDR control.

39. Trunks

Print program – Terminal Number Block Program LD 20

Guidelines – Enter the TGAR information on the TGAR matrix for trunks, DISA DNs, Authcodes, and telephones. If night numbers are Meridian Mail Voice Menu DNs, ensure that the Meridian Mail Voice Menu table for Voice Security Options blocks all unauthorized access. Ensure that the NCOS, TGAR, and CLS are restrictive enough to prohibit direct access to other outbound trunks and long distance calling. Unless trunks tandem through the system for either a network hop-off application or on-net ESN call, the trunks must not have the ability to direct access to other outbound facilities.

Parameter	**Current value**	**Proposed value**
NCOS	_____	_____
NITE	_____	_____
ATDN	_____	_____
TGAR (TIE trunks)	_____	_____
FCAR	Yes No (circle one)	Yes No (circle one)
CLS	_____	_____

See Trunk Administration Program LD 14. These new trunk configuration parameters will be in effect when implementing trunk-related security features.

Auditing Meridian Mail security features

Meridian Mail security features include features that access Meridian Mail mailboxes, voice menus, or automated attendants. To audit an existing Meridian Mail security system, use the Meridian Mail audit checklist.

Meridian Mail audit checklist

The checklist is organized first by software release and then by feature. Each feature is divided into:

- **Print program/print screen –** The name of the program used to print data about the feature. Mailbox information is obtained by using the print screen routine for each mailbox screen of information.
- **Guidelines –** Instructions on filling out proposed values.
- **Parameter values –** Current feature values and proposed feature values.
- The chapter to go to or the program to use to implement any proposed values.

See Voice Security Option screen.

To fill out each feature in the checklist, do the following:

1. Identify the software release.
2. Print out data about the feature using the **Print screen** information.
3. Fill in the **Current values** column using the information generated by the **Print screen**.
4. Use the **Guidelines** to fill out the **Proposed value** column. If keeping the current value, enter a check mark in this column.
5. Refer to the **Implementation** information to implement the **Proposed values**.

1. Call Answering/Express Message Outcalling Thru-dial

Print – Voice Security Option screen

Guidelines – Ensure that all direct Trunk Access Codes, Special Prefix Codes, and AC1 and AC2 codes on system printouts are included in the restriction tables.

On-Switch

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Local

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Long Distance 1

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Long Distance 2

Permission	**Restriction**	**Permission**	**Restriction**
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

See Voice Security Option screen.

2. Directory Number Table

Print – Voice System Administration screen

Guidelines – List all Voice Menu DNs. Compare to the ACD-DNs on the system printouts. Be certain to identify all possible accesses to voice mail. Ensure that Voice Menu Thru-dial restrictions control access to Trunk Access Codes, and SPRE and AC1 and AC2 codes.

See Voice System Administration screen.

3. Express Messaging Thru-dial

Print – Voice Security Option screen

Guidelines – Review permission/restriction tables for each Voice Menu. Ensure that the restriction table for Voice Menus includes blocking of Trunk Access Codes and SPRE and AC1 and AC2 codes.

Menu Name_____

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

See Voice Security Option screen.

4. Passwords

Print – Voice Security Option screen

Parameter	Current value	Proposed value
Invalid log-on attempts	_____	_____
Minimum password length	_____	_____
Forced password change	_____	_____
Number of entries before repeat password	_____	_____
Expiration warning message parameters	_____	_____

See Voice Security Option screen.

5. Password parameters

Print – Voice Security Option screen

Guidelines – When configuring new mailboxes, it is preferable not to use the default password. It is recommended to use the custom password that can be assigned for each mailbox by the system administrator. Users frequently do not change default passwords. Unauthorized persons try the obvious first (default passwords) and then common choices such as 123456, 654321, 222222, 333333 as well as telephone numbers, addresses, and so on.

Parameter	Current value	Proposed value
Invalid log-on attempts per mailbox	_____	_____
Invalid log-on attempts per session	_____	_____
Minimum password length	_____	_____
Forced password change	_____	_____
Number of entries before repeat password	_____	_____
Expiration warning message parameters	_____	_____

See Voice Security Option screen.

6. Thru-dial

Print – Voice Security Option screen

Guidelines – Ensure that all access codes on the system printouts are included in this table. Verify that all direct Trunk Access Codes, Special Prefix Codes, and AC1 and AC2 codes are covered in this table.

Parameter	Current value	Proposed value
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____
Thru-dial restrictions	_____	_____

See Voice Security Option screen.

7. Voice Menu Thru-dial

Print – Voice Security Option screen

Guidelines – Review permission/restriction tables for each Voice Menu. Ensure that the restriction table for Voice Menus includes blocking of Trunk Access Codes and SPRE and AC1 and AC2 codes.

Menu Name_____

Current value		**Proposed value**	
Permission	**Restriction**	**Permission**	**Restriction**
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

See Voice Security Option screen.

Auditing Application Processor security features

System Application Processor security features prevent unauthorized access to the Application Processor console and any terminals and personal computers that could be linked to the Application Processor. This is primarily accomplished through proper password management at the Application Processor and peripheral devices connected to it. Nortel Networks Application Processors are UNIX V based modules, which follow the UNIX basic user ID convention. It supports four user ID Levels. These are:

- **root** – First-Level user ID used by authorized engineering and development personnel only. The **root** user ID is set during an application installation and is chosen based on the ID of the system to which it is connected. The **root** ID is different for each application.
- **disttech** – Second-Level user ID used by qualified field technicians, emergency technical assistance and service, and distributors to configure the Application Processor according to the customer applications requirements. This is also the second-Level default password. The administrator must change this password when the system is first placed in service.

- **maint** or **mlusr –** Third-Level user ID used by the customer application and maintenance administrator to install, modify, and remove applications running on the Application Processor. This is also the third-Level default password.
- **mlusr** and **ccrusr** – Application access user ID. Fourth-Level user ID used by the application user to access the Application Processor console or local or remote terminals and personal computers to run applications. This is also the fourth-Level default password. **ccrusr** is present only if CCR is installed**.**

Obtain a list of all passwords accessing an Application Processor from the first to the fourth Level. Make sure that default passwords are not being used. This is especially critical for the first-Level password, which has access to all Application Processor functions.

System security features verification

Contents

This section contains information on the following topics:

Introduction. 166

Verify system security features using the checklist. 166

New system security verification. 167

Existing system security verification. 167

Verify Call Forward access restrictions. 167

Call Forward External (CFXA/D). 167

Call Forward to Trunk Access Code (CFTA). 168

Verify DISA access restrictions. 168

DISA access using basic restrictions. 168

DISA access using a Security Code (SCOD). 168

DISA access using an Authcode. 169

Verify BARS/NARS access restrictions. 169

Supplemental Digit Recognition/Restriction (SDRR). 169

NCOS/FRL access restrictions. 170

Authorization Code Conditionally Last (NAUT). 170

Time-of-Day Routing (TOD). 170

Routing Control (RTCL). 171

Incoming TIE Trunk Exclusion (ITGE). 171

Verify administration program access restrictions. 171

Administration passwords. 171

Application Processor User ID. 172

Verify Thru-dial restrictions for mailboxes and menus. 172

Thru-dial restrictions. 173

Thru-dial to Voice menus. 173
Express Messaging. 173
Outcalling. 174
Operator Revert. 174
Automated Attendant. 174

Introduction

This chapter describes how to verify that system security is operating properly after it is implemented in the system and Meridian Mail. It provides general guidelines to verify those system security features that most impact the telecommunications facilities. However, the customer is encouraged to use their own system configuration scenarios to verify if their security features have been implemented correctly and are effective.

The most effective method of checking the security of the system is performing the following procedures:

- Verify system security features using the checklist
- Verify Call Forward access restrictions
- Verify DISA access restrictions
- Verify BARS/NARS access restrictions
- Verify administration program access restrictions
- Verify Thru-dial restrictions for mailboxes and menus

Verify system security features using the checklist

To make sure that the required system security has been correctly implemented, compare the system printouts after security features have been implemented with the appropriate checklist for the new or existing system security.

New system security verification

The security installation checklist is used together with new system configuration planning to properly coordinate system security features with the creation of the customer configuration database. Security features selected on this checklist must have been implemented using the system administration overlays.

Verify that all security features selected on the security installation checklist have been implemented by comparing new system printouts against the checklist.

Existing system security verification

The security audit checklist is used to check existing system security features and to specify changes to features that must be upgraded. Any security feature selected for upgrade on this checklist must have been implemented using system configuration programs.

Verify that all security features that were added or selected for upgrade on the security audit checklist have been implemented by comparing the new system printouts against the checklist.

Verify Call Forward access restrictions

Verify the operation of the following Call Forward access restrictions:

- Call Forward External Deny
- Call Forward to Trunk Access Code

Call Forward External (CFXA/D)

To verify the operation of this feature:

- Place an external call to a telephone forwarded to an external number and specified as CFXA. The call should go through.
- Place an external call to a telephone forwarded to an external number and specified as CFXD. The call should not go through.

Call Forward to Trunk Access Code (CFTA)

To verify the operation of this feature:

- Forward a telephone with a DID number to a Trunk Access Code. The telephone should be TGAR 0 or allow direct access to external trunking facilities. Call Forward must be set to a number larger than the ACOD. If CFTA in the customer data block is set to **Yes**, the call should go through.
- Forward the same telephone to the same Trunk Access Code. If CFTA in the customer data block is set to **No**, the call should not go through.

Verify DISA access restrictions

Depending on how security features are implemented for DISA calls, choose one of the following tests:

- DISA access using basic restrictions
- DISA access using a Security Code
- DISA access using an Authorization Code

DISA access using basic restrictions

To verify the operation of this security feature:

- Place a long distance call to a DISA number whose NCOS/TGAR/FRL allows long distance calling. The call should go through.
- Place a long distance call to a DISA number whose NCOS/TGAR/FRL does not allow long distance calling. The call should not go through.

DISA access using a Security Code (SCOD)

To verify the operation of this security feature:

- Place a long distance call using an SCOD from a DISA number whose NCOS/TGAR/FRL allows DISA calling. The call should go through.
- Place a long distance call using an SCOD from a DISA number whose NCOS/TGAR/FRL does not allow DISA calling. The call should not go through.

DISA access using an Authcode

To verify the operation of this security feature:

- Place a noninternational long distance DISA call using an Authcode allowed to access long distance but not international calls. The call should go through if it is not an international call.
- Place an international long distance DISA call using an Authcode allowed to access long distance but not international calls. The call should not go through.

Verify BARS/NARS access restrictions

The system provides many security features to prevent unauthorized BARS/NARS access. The most important of these features must be verified for proper operation. They are:

- Supplemental Digit Recognition/Restriction
- NCOS/FRL access restriction
- Authorization Code Conditionally Last
- Time-of-Day Routing
- Routing Control
- Incoming TIE Trunk Group Exclusion

Supplemental Digit Recognition/Restriction (SDRR)

To verify the operation of this security feature:

- Place a call to an internal telephone dialing the AC1/AC2 and full 7-digit public telephone number. The unnecessary digits are stripped and the extension number is used to reach the destination. The call should go through.
- Place a long distance 976 call from a telephone to an area code denying 976 dialing. The call should not go through.

NCOS/FRL access restrictions

To verify the operation of this security feature:

- Place a call from a telephone by dialing the BARS/NARS access code. If the FRL of the telephone is equal to or greater than the minimum required FRL for the BARS/NARS trunk group, the call should go through.
- Place a call from a telephone by dialing the BARS/NARS access code. If the FRL of the telephone is less than the minimum required FRL for the BARS/NARS trunk group, the call should not go through.
- Place a call from a TIE trunk using an Authcode. If the FRL of the Authcode is equal to or greater than the minimum required FRL for the BARS/NARS trunk group, the call should go through.
- Place a call from a TIE trunk using an Authcode. If the FRL of the Authcode is less than the minimum required FRL for the BARS/NARS trunk group, the call should not go through.

Authorization Code Conditionally Last (NAUT)

To verify the operation of this feature:

- Place a toll call using a telephone that meets minimum FRL requirements for a route list. The call should go through without a request for an Authcode.
- Place a toll call using a telephone that does not meet minimum FRL requirements for a route list. The user should hear a tone or recorded message requesting that an Authcode be entered to complete the call.

Time-of-Day Routing (TOD)

To verify the operation of this feature:

- Place a call during regular business hours to a destination that is restricted during off hours. The call should go through.
- Place a call after regular business hours to a destination that is restricted during off hours. The call should not go through.

Routing Control (RTCL)

To verify the operation of this feature:

- Place a call during regular business hours from a telephone with a specified NCOS/FRL able to access WATS and CO trunks during normal business hours. The call should go through.
- Place a call from the same telephone after RTCL goes into effect. The call should not go through.

Incoming TIE Trunk Exclusion (ITGE)

To verify the operation of this feature:

- Place a call from a remote location by directly accessing a TIE route; dial a number that is not restricted in the remote PBX's translation table and in the local system's ITGE table. The call should go through.
- Place a call from a remote location by directly accessing a TIE route; dial a number that is restricted in the remote PBX's translation table and in the local system's ITGE table. The call should not go through.

Verify administration program access restrictions

To verify system and Application Processor administration passwords and user IDs, perform the following tests:

- Verify administration passwords
- Verify Application Processor User ID

Administration passwords

To verify the operation of this feature:

- Log on to the system console using the Level 1 password, load LD 17, and try to change the Level 2 password. The program should not display the PWD2 prompt on the screen, thus restricting access to the password change privilege.

- Log on to the system console using the Limited Access to Overlay Level 1 password and load LD 17. LD 17 should not load if the password is configured to restrict access to LD 17.
- Try to log on to the system console using an invalid password until the threshold value is reached. The port should lock out and the other maintenance TTYs on the system should receive a message detailing the log-on attempts. Log on to another port using the Level 2 password. A special message should be displayed regarding invalid log-on attempts. Access the Audit File to verify that there is a history of invalid log-on attempts.

Application Processor User ID

To verify the operation of this feature:

- Log on to the Application Processor console using a valid Level-four user ID. It should be possible to log on and run applications. However, it should not be possible to modify, install, or remove an application using this user ID.
- Log on to the Application Processor using the other three Levels of user IDs and verify that the features accessible to each user ID can actually be accessed and those restricted cannot be accessed.
- Log on to the Application Processor console using an invalid user ID. It will not be possible to log on. Try to log on using an invalid user ID until the system refuses to display the log-on prompt. The number of permitted unsuccessful logons can be set. This number is usually set at 3.

Verify Thru-dial restrictions for mailboxes and menus

To verify Meridian Mail security features, perform the following tests:

- Verify Thru-dial restrictions
- Verify Thru-dial to Voice menus
- Verify Express Messaging
- Verify Outcalling

- Verify Operator Revert
- Verify Automated Attendant

Thru-dial restrictions

To verify the operation of this feature:

- Place a call to a telephone that performs a Forward No Answer to Meridian Mail. When Meridian Mail answers, dial 0 followed by an extension number or an access code and telephone number that is permitted to Thru-dial followed by the # sign. The call should go through.
- Place a call to a telephone that performs a Forward No Answer to Meridian Mail. When Meridian Mail answers, dial 0 followed by an extension number or an access code and telephone number that is restricted to Thru-dial followed by the # sign. The call should not go through.

Thru-dial to Voice menus

To verify the operation of this feature:

- Using the **Voice Security Option** screen, specify the permission/restriction table to define the numbers allowed to be accessed and those restricted from access.
- Dial 0 followed by an extension number or an access code and telephone number that is permitted to Thru-dial followed by the # sign. The call should go through.
- Dial 0 followed by an extension number or an access code and a telephone number that is restricted to Thru-dial followed by the # sign. The call should not go through.

Express Messaging

To verify the operation of this feature:

- Set a permission/restriction table for Meridian Mail access using the express messaging feature.

- Dial a number that is permitted to access Meridian Mail directly. The access should be direct and it should not be necessary to dial a user's directory number.
- Dial a number that is not permitted to access Meridian Mail directly. To access Meridian Mail, it is necessary to dial a user's directory number and then be forwarded to Meridian Mail.

Outcalling

To verify the operation of this feature:

- Define where the messages should be sent for non-user telephones.
- Access the Meridian Mail mailbox and enter the SEND command. Meridian Mail should dial the non-user telephone and deliver the messages when it detects voice, or when the non-user presses 2 if prompted.
- Listen to the message, record a reply, and forward it to the sender. The reply should automatically be deposited in the sender's mailbox.

Operator Revert

To verify the operation of this feature:

- Using the **Modify User** screen, define permission/restriction tables to specify an Operator Revert DN for each mailbox.
- Access a mailbox. Activate the Operator Revert feature, if configured for that mailbox, by dialing 0 while listening to the greeting or after leaving a message. The call will automatically be forwarded to the predetermined Operator Revert DN.

Automated Attendant

To verify the operation of this feature:

- Define a permission/restriction table for DISA or self-terminating numbers that are allowed or denied access to the automated attendant.
- Dial a DISA or a self-terminating call to the automated attendant. If the number dialed is allowed, it should be forwarded by the automated attendant; if the number is denied, it will terminate at the automated attendant.

System security analysis

Contents

This section contains information on the following topics:

Introduction. 176
Using the system reports summary. 176
Analyzing Call Detail Recording reports. 178
Analyzing Traffic Measurement reports. 182
Network traffic reporting (TFC001). 183
Trunk traffic reporting (TFC002). 185
Percent All Trunks Busy reporting (TFC104). 187
Long-duration call reporting (TFS40X and TFS41X). 189
Routing measurements (TFN001). 190
Network Class of Service measurements (TFN002). 193
Checking the History File. 195
Analyzing Operational Measurement reports. 196
Monitoring Outcalling activities 196
Monitoring Outcalling activities. 197

Reference list

The following are the references in this section:

- *Traffic Measurement: Formats and Output* (553-2001-450)
- *Call Detail Recording: Description and Formats* (553-2631-100)

Introduction

This chapter describes how to analyze system security to detect unauthorized access and fraud, using system reporting capabilities. The most effective method of detecting fraud is by doing the following:

- using the system reports summary
- analyzing Call Detail Recording reports
- analyzing Traffic Measurement reports
- checking the History File
- analyzing Operational Measurement reports

The information in this chapter must be used as part of routine system maintenance after security has been implemented and security features are operating correctly. It can reveal unauthorized call placements, unusual traffic patterns, and past events and system messages that can reveal unauthorized or attempted access to the system.

Using the system reports summary

There are a number of messages and reports that can be used to analyze security for the system. Table 43 on page 177 provides a summary of these messages and reports. Table 43 shows how they can help analyze fraud using the statistics they provide, and how they are obtained. Use this summary to find the reports that will produce the needed information. These reports are discussed in detail in this chapter.

The History File includes a separate file dedicated to traffic. Reports can be sent to that file instead of to the online printer.

Table 43
System reports summary (Part 1 of 2)

Information required	Report	Statistics provided	Output
Call placement statistics per telephone.	CDR	Identifies the calling party, trunk group used, destination called, the time, date, and duration of the call, and the Authcode or account code used to place the call.	To devices as defined.
Trunk-to-trunk call activity.	TFC001	The tandem peg count and usage.	According to schedule.
Individual trunk group activity including All Trunks Busy conditions.	TFC002	The peg count and usage for both incoming and outgoing calls, and peg count of All Trunks Busy conditions.	According to schedule.
All Trunks Busy conditions violating specified threshold.	TFC104	All Trunks Busy conditions on a per route basis if established threshold is exceeded.	Automatically to a maintenance TTY if All Trunks Busy conditions exceed threshold. Associated trunk group report is also output according to its schedule.
Long call duration information.	TFS401 and TFS402	TFS401 and TFS402 identify the terminal numbers (TNs) involved in connections 36 to 49 CCS and 50 CCS or higher, respectively.	According to schedule.
	TFS411 and TFS412	TFS411 and TFS412 provide a peg count and total CCS of connections 36 to 49 CCS and 50 CCS or higher, respectively.	According to schedule.

Table 43
System reports summary (Part 2 of 2)

Information required	Report	Statistics provided	Output
Call activity by Route List NCOS using BARS/NARS.	TFN001	The peg count by Route List of how often the Route List was accessed and the number of calls that were successfully completed.	According to schedule.
NCOS call activity through BARS/NARS.	TFN002	The number of call attempts each NCOS group generated and other statistics.	According to schedule.
How often a service such as Thru-dial and Outcalling is used.	Voice Service Summary	The number of times callers used a service and the average length of each call.	On demand.
Outcalling activity for incoming and outgoing calls.	Outcalling Detail	The number of requests, attempts, retries, and the average wait time Outcalling was used.	On demand.

Analyzing Call Detail Recording reports

Call Detail Recording (CDR) reports show the details of a call, such as called and calling parties, time and duration of the call, and access codes used to place the call. Among the signs of fraudulent use are calls placed to international or unauthorized locations, calls of unusually long duration, and calls placed during nonbusiness hours.

The system outputs a record when a call terminates, when a user enters a valid Authcode or charge account code, or when a call is modified. The following types of trunk and telephone calls can be selected to appear in the CDR report:

- Incoming trunk calls
- Outgoing trunk calls

- Outgoing toll trunk calls
- Internal telephone-to-telephone calls

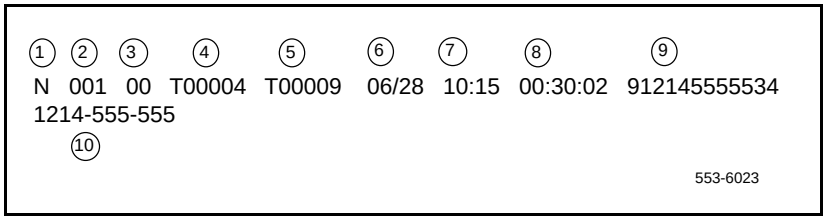
Table 44 shows how to configure CDR and print reports for customers, routes, Authcodes, and telephones.

Table 44
Configuring and printing CDR reports

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB, ADAN, USER = CTY	LD 22 CFN or LD 22 ADAN
Customer	LD 15 - CDR = YES, AXID, TRCR, CDPR, PORT	LD 21 by CUST or LD 21 Data groups
Route - enabled on a per route basis	LD 16 - CDR = YES, INC, OAL, QREC, OTL, AIA, OAN, NATL, TDG, OPD	LD 21 by Route
Authcode	LD 88 - ACDR = YES	LD 88 by AUB
Telephones	LD 10 and LD 11 - CLS	LD 20 by TN LD 10/11 by TN LD 81 by FEAT = ICDA, ICDD

Figure 1 shows an example of the CDR report. The circled numbers correspond to the description of fields below Figure 1. For other CDR report examples, see *Call Detail Recording: Description and Formats* (553-2631-100).

Figure 1
Call Detail Recording record example



1 Record Type – The type of call record being output. This field consists of a letter identifying the type of record:

N Normal – Generated when a user places a regular call and does not activate other telephone features.

S Start – Generated when one of the following features affect a call: Call Transfer, Conference, Call Forward, Barge-In, Busy Verify, Privacy Release, or Override.

E End – Generated when a call terminates, which is associated with a specific start record.

A Authorization Code – Generated when a user enters an Authcode and does one of the following:

— makes a trunk call

— calls a local telephone to make a DISA call

— activates Ring Again

This must be set in the Authcode data block to appear on the CDR report.

C Charge Account – Generated when a user enters a charge account code and makes a trunk call or has already established a call.

M Charge for Conference – Generated when a user enters a charge account code during a conference call. This record allows for each conference party to be charged with a different charge account code, if necessary.

Q Initial Connection – Generated when an ACD agent makes or receives a trunk call.

R Transfer Connection – Generated when an ACD agent transfers a call.

F Conference Connection – Generated when an ACD agent sets up a conference call.

L Internal Call Record – Generated when a telephone completes an internal call.

2 **Record Number –** The number of the current record in the CDR sequence.

3 **Customer Number** – The customer associated with the call.

4 **Originator Identification –** The facility that originated the call:

DNxxxx	Telephone
ATTNxx	Attendant
CFlllnn	Conference
Txxxxxx	Trunk without answer supervision
Axxxxxx	Trunk with answer supervision

5 **Terminator Identification –** The facility on which a call terminated:

DNxxxx	Telephone
ATTNxx	Attendant
CFllln	Conference
Txxxxxx	Trunk without answer supervision
Axxxxxx	Trunk with answer supervision

6 **Timestamp (Date and Time) –** The date and time of a call. Its exact definition depends on the type of record:

N	For a normal record, it shows when a call ends.
I	For an internal record without call modification, it shows when the call ends.
I	For an internal record with call modification, it shows when the call has been modified.
S	For a start record, it shows when the call begins.
E	For an end record, it shows when the call ends.
Q, R, F	For a connection record, it shows when the call is connected.

7 **Call Duration** – The length of time the call lasted.

8 **Digits Dialed** – The telephone number dialed.

9 **CLI/ANI Digits** – The telephone number of the calling party, which appears in the report only if this option is installed.

Analyzing Traffic Measurement reports

Traffic Measurement reports are used to monitor the traffic volume and variations in the traffic volume that can indicate possible unauthorized use. These reports can be printed on-demand or according to a schedule. Among the signs of fraudulent use are increased trunk-to-trunk activity, long call durations, and calls to unusual locations.

Table 45 shows how to configure traffic output ports and set up an automatic report printing schedule.

Table 45
Configuring traffic output ports and schedule

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB = YES, ADAN, USER = TRF	LD 22 by CFN or LD 22 by ADAN
Traffic	LD 2 - SSHC	LD 2 - TSHC

Network traffic reporting (TFC001)

Traffic measurements provided by the TFC001 report include a cumulative peg count and information about incoming, outgoing, and tandem trunk activity. Of particular value in identifying possible fraudulent activity are the tandem (trunk-to-trunk) CCS and peg count.

Table 46 shows prompts in Traffic Program LD 2 to configure and print the TFC001 report.

Table 46
Configuring and printing the TFC001 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPS	LD 2 TOPS

Figure 2 is an example of the TFC002 report showing trunk-to-trunk CCS and peg count for tandem calls processed during the reported period. The circled numbers correspond to the description of fields below Figure 2.

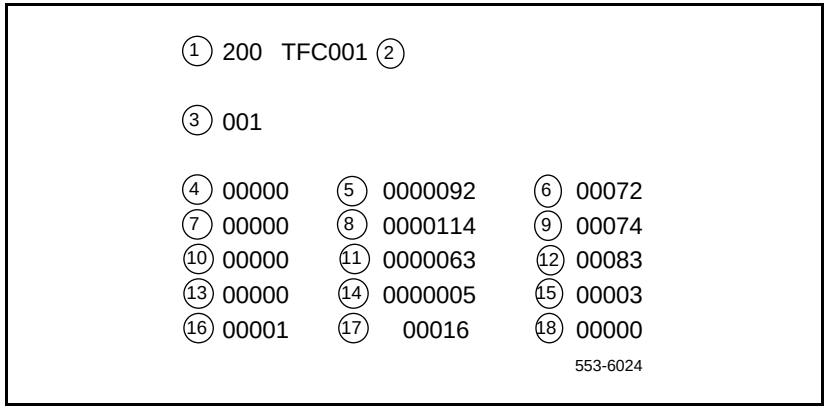
1 **System ID –** the number assigned to the system for a specific site.

2 **Report Name –** the name of the report.

3 **Customer Number –** the customer associated with the call.

4 **Incoming FTM –** the number of incoming FTMs.

Figure 2
TFC001 report example



5 Incoming CCS – the amount of time in hundred call seconds (CCS) for incoming trunk calls.

6 Incoming PC – the number of incoming trunk calls processed.

7 Outgoing FTM – the number of outgoing FTMs.

8 Outgoing CCS – the amount of time in hundred call seconds (CCS) for outgoing trunk calls.

9 Outgoing PC – the number of outgoing trunk calls processed.

10 Intra-Customer FTM – the number of internal FTMs processed.

11 Intra-Customer CCS – the amount of time in hundred call seconds (CCS) for internal calls.

12 Intra-customer PC – the number of internal calls processed.

13 Tandem FTM – the number of tandem FTMs processed.

14 Tandem CCS – the amount of time in hundred call seconds (CCS) that trunk-to-trunk connections were held.

15 Tandem PC – the number of trunk-to-trunk calls processed.

Note: Tandem CCS and Tandem PC are of particular value in identifying possible fraudulent activity.

16 **Permanent Signal –** the number of trunks that are in permanent signal mode.

17 **Abandon –** the number of calls that were not completed.

18 **Partial Dial** – the number of calls that did not complete the dialing sequence.

Trunk traffic reporting (TFC002)

TFC002 provides information about use, overflow, and All Trunks Busy (ATB) conditions for each trunk group. Signs of fraud include All Trunks Busy conditions, a higher than normal amount of call activity, and high usage occurring outside of normal business hours.

TFC002 can be a scheduled report, but the system generates the TFC002 report automatically when an All Trunks Busy threshold violation occurs during the reporting period, regardless of whether the report is scheduled or not.

TFC002 includes a Traffic Period Option and a Trunk Seizure Option. These options can be selected in the Configuration Data Block. Refer to *Traffic Measurement: Formats and Output* (553-2001-450) for more information.

Table 47 shows the prompts in Traffic Program LD 2 to configure and print the TFC002 report.

Table 47
Configuring and printing the TFC002 report

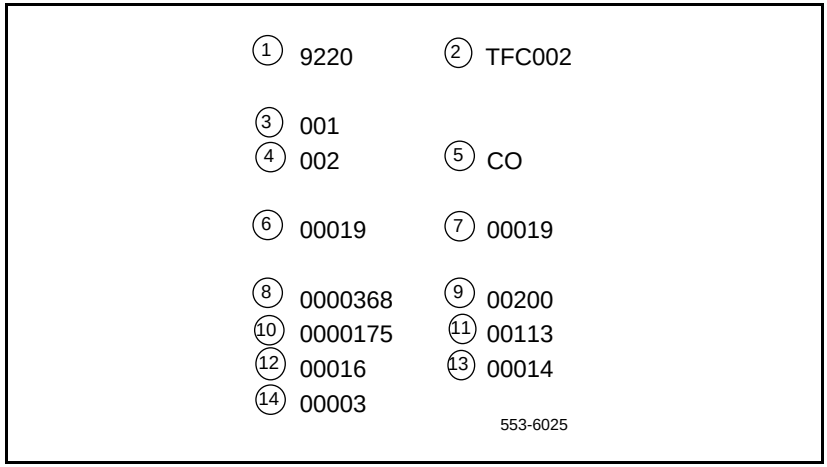
Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPC	LD 2 TOPC

Figure 3 is an example of the TFC002 report that is automatically generated when an All Trunks Busy condition is reached. The circled numbers correspond to the description of fields.

1 **System ID –** the number assigned to the system for a specific site.

2 **Report Name –** the name of the report.

Figure 3
TFC002 report example



3 **Customer Number –** the customer associated with the call.

4 **Route Number –** the Route Number that is the subject of the report.

5 **Trunk Type –** the type of trunk group, which can be CO=Central Office, WATS=Wide Area Telephone Service, DID=Direct Inward Dial, TIE=TIE Line, FEX=Foreign Exchange.

6 **Trunks Equipped** – the number of trunks in the system.

7 **Trunks Working –** the number of trunks that are operating in the system.

8 **Incoming Usage** – the total time in hundred call seconds (CCS) that incoming calls lasted on trunks in the trunk group.

Note: Look for and investigate a higher than normal amount of incoming trunk traffic.

9 **Incoming PC –** the number of incoming calls processed on the trunk group.

10 **Outgoing Usage –** the total time in CCS that outgoing calls lasted on trunks in the trunk group.

11 **Outgoing PC** – the number of outgoing calls processed on the trunk group.

Note: Look for and investigate a higher than normal amount of outgoing trunk traffic.

12 **Outgoing Overflow** – the number of times all trunks in this trunk group were busy when a user tried to gain access to the route and the system blocked the attempt or routed the call over an alternate route.

13 **All Trunks Busy –** the number of times all trunks in this route were busy, whether a user tried to gain access or not.

Note: Look for and investigate a higher than normal number of overflows and All Trunks Busy conditions.

14 **Toll PC –** the number of times that toll calls (0+ or 1+ calls) were established on Central Office (CO) and Foreign Exchange (FX) trunk routes.

Note: Look for and investigate a higher than normal number of toll calls.

Percent All Trunks Busy reporting (TFC104)

TFC104 is an All Trunks Busy report that allows the percent of time an All Trunks Busy condition occurs for a customer to be set. When call activity exceeds the percentage threshold during the reporting period, the system automatically outputs the report.

This report identifies the trunk group, the All Trunks Busy percentage for the trunk group, and the percentage threshold value.

The associated trunk group report (TFC002) is also automatically output at its scheduled report time.

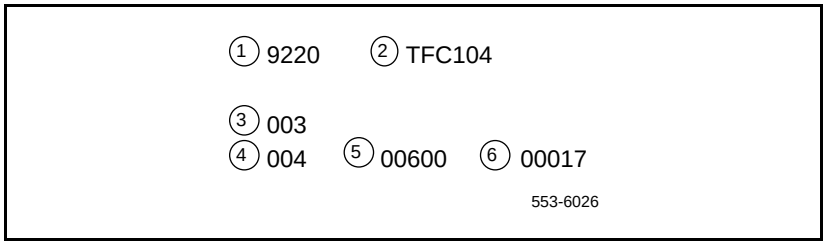
Table 48 shows Traffic Program LD 2 prompts used to configure and print the TFC104 report.

Table 48
Configuring and printing the TFC104 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 STHC	LD 2 TTHC

Figure 4 is an example of the TFC104 report that is automatically generated when an All Trunks Busy condition is reached. The circled numbers correspond to the description of fields following Figure 4.

Figure 4
TFC104 report example



1 **System ID –** the number assigned to the system for a specific site.

2 **Report Name –** the name of the report.

3 **Customer Number** – the customer number to which the trunk group belongs.

4 **Trunk Group –** Trunk Group Number that is the subject of the report.

5 **Busy –** indicates the All Trunks Busy percentage that occurred in units of 0.1 percent.

Note: Look for and investigate a higher than normal number of All Trunks Busy conditions.

6 **Threshold –** indicates the All Trunks Busy threshold for this customer in units of 0.1 percent.

Long-duration call reporting (TFS40X and TFS41X)

TFS40X messages are output to the traffic terminal at regularly scheduled intervals showing long-holding connections.

Messages such as TFS401 and TFS402 are displayed to show the number of calls that exceeded the specified call duration threshold.

TFS411 and TFS412 are output at regularly scheduled intervals showing the total number of calls that exceeded the specified call duration threshold. These messages help you to monitor calls of unusually long duration.

TFS401 output automatically identifies the Terminal Numbers (TNs) of connections held for at least 36 hundred call seconds (CCS) but less than 50 CCS.

TFS411 provides a peg count of the number of connections held for at least 36 CCS but less than 50 CCS, together with total use on the connections.

TFS402 output automatically identifies the TNs of connections that were held for 50 CCS or longer.

TFS412 provides a peg count of the number of connections that were held for 50 CCS or longer, together with the total use on the connections.

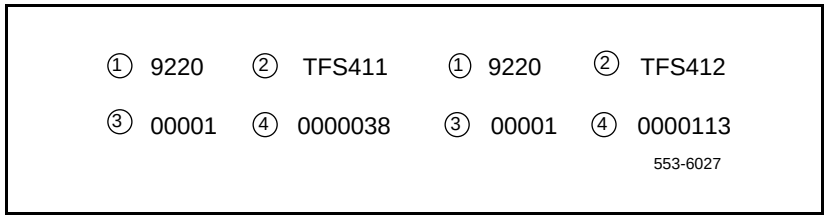
Table 49 specifies Traffic Program LD 2 prompts used to configure and print the TFS40X messages.

Table 49
Configuring and printing TFS40X messages

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPC	LD 2 TOPC

Figure 5 is an example of the TFS411 and TFS412 reports. The circled numbers correspond to the description of fields below Figure 5.

Figure 5
TFS411 and TFS412 messages example



1 **System ID –** the number assigned to the system for a specific site.

2 **Message Name –** the name of the message.

3 **Number of Connections –** the number of calls that were held for the peg count of the report.

4 **Total Usage (CCS) –** the total amount of time all calls were held.

Note: Look for and investigate a higher than normal number of long call durations on trunk-to-trunk calls.

Routing measurements (TFN001)

TFN001 provides data related to individual Route List use. For each Least Cost Route List, the report shows how often the list was accessed, which entries in the list were used, and whether callers were successful in completing a selection.

By partitioning “high fraud” numbers into unique route list indexes, activity can be tracked more effectively. The report can show calls to international locations and 900 numbers, indicating possible unauthorized access.

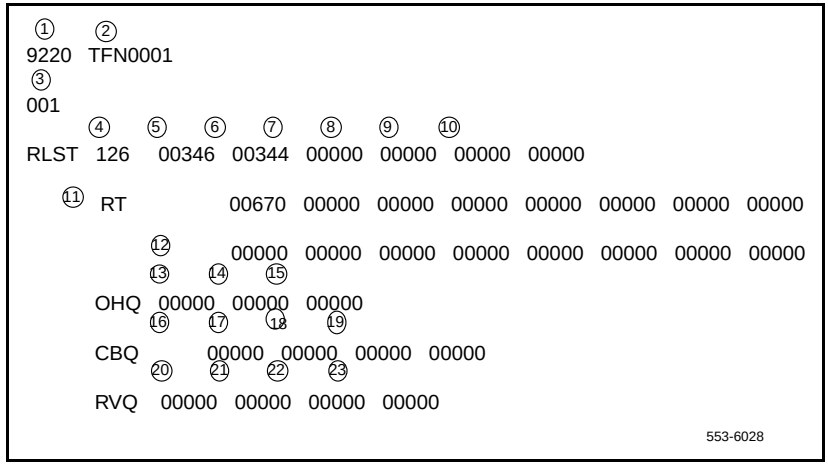
Table 50 shows Traffic Program LD 2 prompts to configure and print routing measurement reports.

Table 50
Configuring and printing the TFN001 report

Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPN	LD 2 TOPN

Figure 6 is an example of the TFN001 showing Route List information that indicates the usage of BARS/NARS and calls blocked by the Route List. The circled numbers correspond to the description of fields following the figure.

Figure 6
TFN001 report example



1 **System ID –** the number assigned to the system for a specific site.

2 **Report Name –** the name of the report.

3 **Customer Number** – the customer number to which the trunk group belongs.

4 **Route List Number –** the Route List number for which the report was generated.

5 **Route List Requests** – the number of times the Route List was chosen to process a call.

6 **Route List Requests Served Without Delay** – the number of calls routed using the Route List that did not encounter any delay.

7 **Expensive Route Acceptances –** the number of times users allowed calls to be completed over expensive routes.

Note: Look for and investigate traffic using expensive routes.

8 **Route List Requests Standard Blocking –** the number of calls blocked at the Route List because routes or queues were not available.

Note: Look for and investigate callers attempting to call specific locations that are blocked.

9 **Not Used**

10 **Not Used**

11 **Route List Entry Usage** – the number of times each entry in the Route List was used.

12 **TD Calls –** the number of long distance calls that used a tone detector dial tone to complete the call.

13 **OHQ Calls –** the number of calls placed in the Off-Hook Queue.

14 **OHQ Average Time –** the average time calls stayed in the Off-Hook Queue in 0.1 seconds.

15 **OHQ Cancellations –** the number of calls that were canceled while waiting in the Off-Hook Queue.

16 **CHQ Calls –** the number of calls placed in the Call-Back Queue.

17 **CBQ Average Time –** the average time calls stayed in the Call-Back Queue in 0.1 seconds.

18 **CBQ Offerings –** the number of calls that were offered Call-Back Queuing.

19 **CBQ Cancellations –** the number of calls that were canceled by the user while waiting in the Call-Back Queue.

20 **RVQ Quantity –** the number of calls placed in the Remote Virtual Queue.

21 **RVQ Average Time –** the average time calls stayed in the Remote Virtual Queue in 0.1 seconds.

22 **RVQ Offerings –** the number of calls that were offered Remote Virtual Queuing.

23 **RVQ Cancellations** – the number of calls that were canceled by the user while waiting in the Remote Virtual Queue.

Network Class of Service measurements (TFN002)

TFN002 provides information about outgoing BARS/NARS activity for each defined NCOS group. The report includes a count of the total number of call attempts each NCOS group generates.

By partitioning users, TIE trunks, and Authcodes into easily identified NCOS groups, normal calling patterns associated with each group can be monitored. Variations in normal calling patterns can be readily noticed.

Table 51 specifies Traffic Program LD 2 prompts used to configure and print the TFN002 report.

Table 51
Configuring and printing the TFN002 report

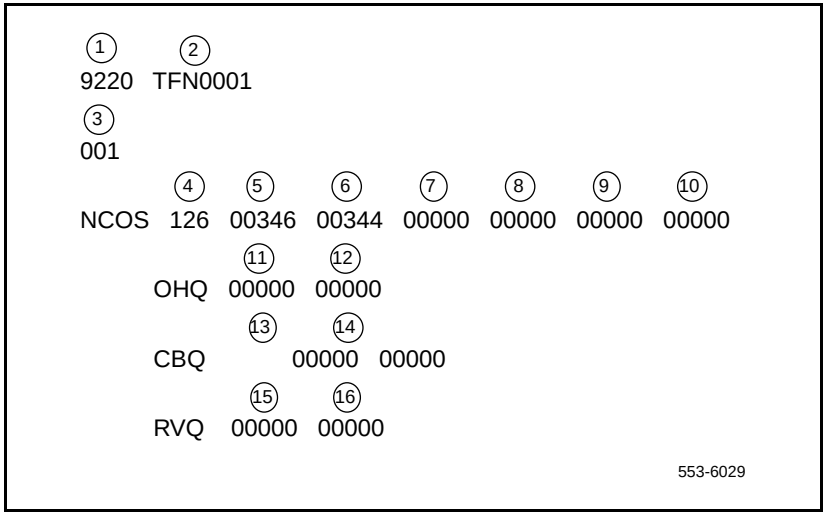
Facility	Overlay and prompts	Print programs
Traffic	LD 2 SOPN	LD 2 TOPN

Figure 7 is an example of the TFN002 report showing the number of attempts a caller with a specific NCOS made during the specified reporting period. The circled numbers correspond to the description of fields below Figure 7.

1 **System ID –** the number assigned to the system for a specific site.

2 **Report Name** – the name of the report.

Figure 7
TFN002 report example



3 **Customer Number** – the customer number to which the trunk group belongs.

4 **NCOS –** the NCOS group shown in the report.

5 **Call Attempts –** the number of calls attempted by the NCOS group.

Note: Look for and investigate excessive number of calls attempted to a specific destination.

6 **Routing Requests Served Without Delay** – the number of calls routed by the network that did not encounter any delay.

7 **Expensive Route Acceptances –** the number of times users allowed calls to be completed over expensive routes.

Note: Look for and investigate traffic using expensive routes.

8 **Network Call Standard Blocking** – the number of calls blocked by the network because routes or queues were not available.

Note: Look for and investigate callers attempting to call specific locations that are being blocked.

9 Not Used

10 Expensive Route Refusals – the number of calls refusing the use of expensive routes.

11 OHQ Calls – the number of calls placed in the Off-Hook Queue.

12 OHQ Average Time – the average time calls stayed in the Off-Hook Queue in 0.1 seconds.

13 CHQ Calls – the number of calls placed in the Call-Back Queue.

14 CBQ Average Time – the average time calls stayed in the Call-Back Queue in 0.1 seconds.

15 CHQ Calls – the number of calls placed in the Remote Virtual Queue.

16 CBQ Average Time – the average time calls stayed in the Remote Virtual Queue in 0.1 seconds.

Checking the History File

Certain system messages or activities can be tracked and printed as required. The History File stores system messages in memory. The stored information can be accessed from a local or remote terminal and printed.

The type of information to be stored in the History File can be specified. This can include Maintenance messages (MTC), Service Change activity (SCH), Customer Service Change activity (CSC), Traffic outputs (TRF), and software error messages (BUG). By storing SCH activity and TRF output messages, information associated with traffic patterns can be retrieved that can reveal unauthorized access to the PBX.

Table 52 on page 196 shows Traffic Program LD 2 prompts used to configure and print specific messages for the History File.

Table 52
Configuring and printing the History File

Facility	Overlay and prompts	Print programs
Configuration	LD 17 - IOTB, HIST, ADAN USER	LD 22 by CFN or LD 22 by ADAN

Analyzing Operational Measurement reports

Operational Measurement reports are generated at the Meridian Mail administration terminal. They provide information about Thru-dial and Outcalling activities that can help locate and prevent fraud.

Monitoring Thru-dial activities

Assess how callers use Thru-dial by reviewing the Operational Measurement Reports– Voice Service Summary. This report lists the number of times callers used a service such as Thru-dial, and the average length of each call. Use this report to determine whether Thru-dial traffic is unusually high for your system. A high amount of Thru-dial tandem traffic could indicate unauthorized use.

Table 53 is an example of the Voice Service Summary report.

Table 53
Voice Service Summary report example (Part 1 of 2)

Operational Measurement				
Voice Service Summary				
Interval Start-End	**Service Name**	**Number of Accesses**	**Average Length (in sec)**	**Meridian Mail Usage (in CCS)**
2/08 9:00 - 10:00	Thru-dial	5	60	3
2/08 9:00 - 10:00	Voice Menu	10	30	3
2/08 9:00 - 10:00	VM Log-on	10	30	3
2/08 9:00 - 10:00	Call Answering	60	30	18

Table 53
Voice Service Summary report example (Part 2 of 2)

Operational Measurement				
Voice Service Summary				
Interval Start-End	**Service Name**	**Number of Accesses**	**Average Length (in sec)**	**Meridian Mail Usage (in CCS)**
2/08 9:00 - 10:00	Express Messaging	10	60	6
2/08 9:00 - 10:00	Voice Announcements	5	60	3
2/08 9:00 - 10:00	Networking	10	60	6
2/08 9:00 - 10:00	Voice Administration	0	0	0
2/08 9:00 - 10:00	Time of Day Control	0	0	0
2/08 9:00 - 10:00	Delivery to Non-users	5	0	0
2/08 9:00 - 10:00	Remote Notification	0	0	3
2/08 9:00 - 10:00	Remote Activation	0	0	0

The following describes the fields in the report. Some of these fields differ slightly depending on the release of software:

- **Interval Start-End** – the start and end time of each reporting interval.
- **Service Name –** the name of the service.
- **Number of Accesses –** the number of direct calls made to each service.
- **Average Length –** the average length of a call in seconds.
- **Meridian Mail Usage –** the amount of time in CCS Meridian Mail service was active.

Monitoring Outcalling activities

Assess the use of the Outcalling features Delivery to Non-users and Remote Notification through the Operational Measurement Reports Voice Service Summary and Outcalling Detail. These reports must be used together to detect excessive use of these features.

The Voice Service Summary lists the number of times a service was used and the average length of service. Use this report to determine if your system is experiencing excessive use of Message Delivery to Non-users and Remote Notification. Such an increase could indicate an unauthorized access problem.

Table 53 on page 196 shows an example of the Voice Service Summary report.

The Outcalling Detail report gives detailed statistics on Outcalling activity for incoming and outgoing calls. This report shows the number of requests, attempts, retries, and the average wait time. Use this report to determine if there is higher than normal Message Delivery to Non-users and Remote Notification tandem traffic for the system. An increase in such traffic could indicate a problem with unauthorized access.

Table 54 is an example of the Outcalling Detail report.

Table 54
Outcalling Detail report example

Operational Measurement										
Outcalling Detail (Remote Notification and Delivery to Non-users)										
	Number of New Requests		Number of Attempts				Number of Successes		Wait Avg	Time Max
			New Requests		Retries					
Interval Start-End	RN	DNU	RN	DNU	RN	DNU	RN	DNU	(sec)	(sec)
2/08 9:00 - 10:00	0	0	0	0	0	0	0	0	0	0
2/08 9:00 - 10:00	1	0	0	0	0	0	1	0	259	259
2/08 9:00 - 10:00	4	0	1	0	0	0	0	0	0	0
2/08 9:00 - 10:00	1	1	0	1	0	0	0	0	0	0

The following describes the fields in the report:

- **Interval Start/End –** the start and end time of the report.
- **Number of New Requests –** the total number of requests the Remote Notification user made to deliver a message to a non-user.
- **Number of Attempts –** the total number of attempts made at Remote Notification and Delivery to Non-users.
- **New Requests –** the number of new requests attempted.
- **Retries –** the number of times the system had to retry Remote Notification or Delivery to Non-users calls because the number was busy or not answered.
- **Number of Successes –** the number of successful Remote Notification and Message Delivery to Non-users calls.
- **Wait Time** – the average time an Outcalling agent took to acquire the necessary resources to call out to the specified DN.

Appendix A: Access Restriction features

Use Table 1 on page 201 to assess the features available that can be used to restrict access. **X** indicates features available that can be used to control each area of access. **Test** indicates features that can be used to assess potential abuse in the areas of access. **Optional** indicates features that may or may not be used to control their area of access.

Table 1
Feature Assessment (Part 1 of 3)

Security Features	DISA	Voice Mail	Internal	Network	System
Class of Service	X	X	X	X	
Trunk Group Access Restrictions	X	X	X	X	
System Speed Call			X		
Authorization Codes	X		X	X	
Sta Spec Authcode			X		X
Forced Charge Account			X	X	
Controlled Class of Service			X		
Enhanced Controlled Class of Service			X		
Flexible Feature Code			X		
Code Restriction			X	X	
New Flexible Code Restriction			X	X	

Table 1
Feature Assessment (Part 2 of 3)

Security Features	DISA	Voice Mail	Internal	Network	System
Call Forward External Deny			X		
Flexible Feature Code - Remote Call Forward			X		
Internal Call FWD			X		X
Call Detail Recording	Test	Test	Test	Test	
Internal Call Detail Recording			Test		
Traffic Measurement	Test	Test	Test	Test	
Supplemental Digit Restriction and Recognition	X		X		
Network Class of Service	X	X	X	X	
Network Speed Call	Optional		Optional	Optional	
Network Authorization Code - Authorization Code Conditionally Last	Optional		Optional	Optional	
Routing Control			X	X	
Incoming Trunk Group Exclusion				X	
Meridian Mail System Options Voice Security		X			
Meridian Mail User Options		X			
Meridian Mail Voice Menus Thru-dial Security		X			
Level 1 Password					X
Level 2 Password					X

Table 1
Feature Assessment (Part 3 of 3)

Security Features	DISA	Voice Mail	Internal	Network	System
Limited Access to Passwords					X
Trunk barring					
Scheduled Access Restrictions					
Restricted Call Transfer					
User Selectable Call Redirection					
Multi-user User Name					Test
Attendant Administration					X
Automatic Set Relocation					X
History File					Test
Password Protection		X			
A/B Switch to Restrict External Access to Administration		X			
Authorization Code					
Alarms					

Appendix B: Trunk Group Access Restrictions worksheet

Use Table 1 on page 206 to specify Trunk Group Access Restrictions (TGAR) for each route. Also, specify the trunk type and access code required to access that route.

Table 1
Trunk Group Access Restrictions worksheet (Part 1 of 4)

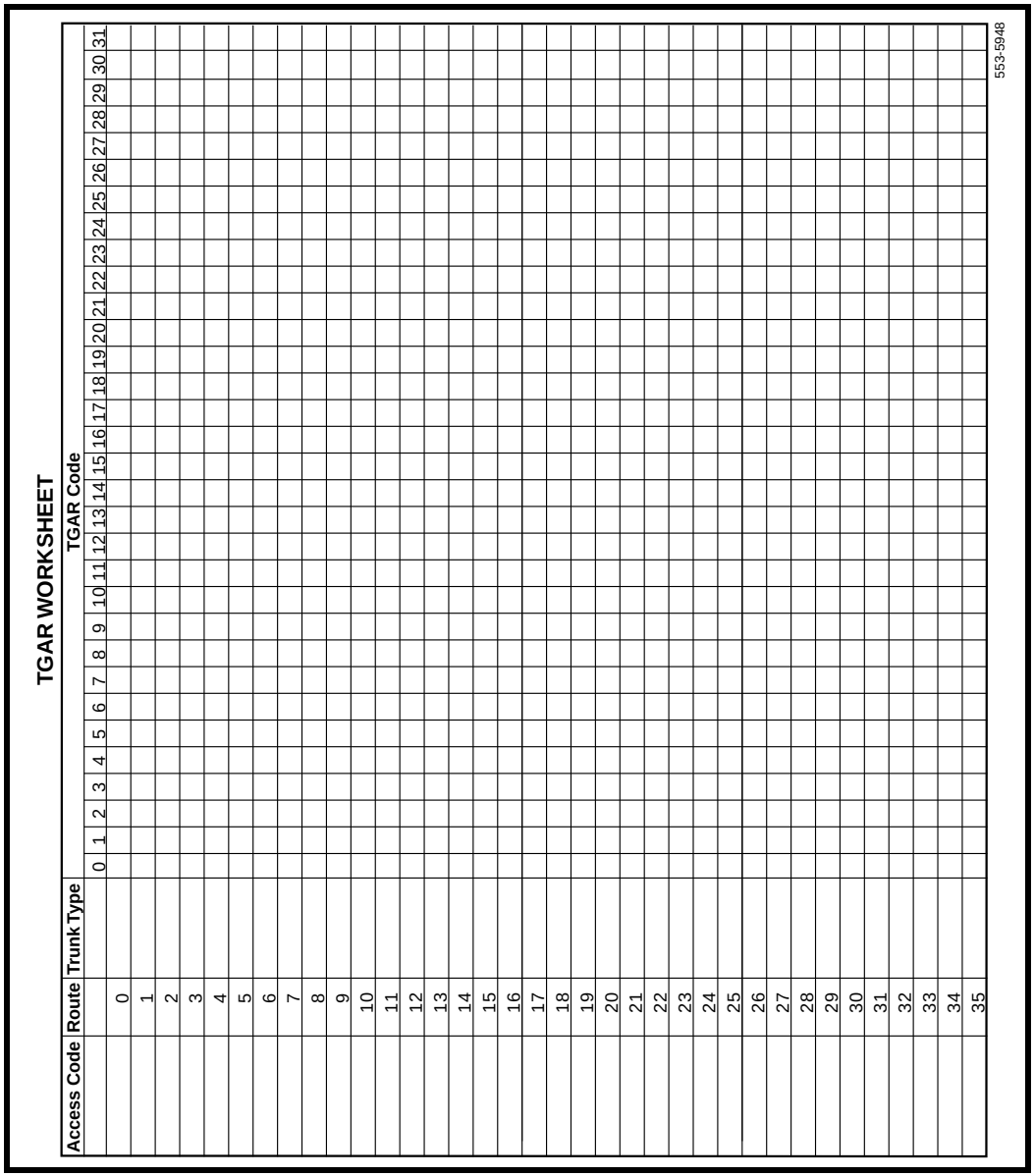


Table 1
Trunk Group Access Restrictions worksheet (Part 2 of 4)

TGAR WORKSHEET

Access Code	Route	Trunk Type	TGAR Code																													
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	36																																	
	37																																	
	38																																	
	39																																	
	40																																	
	41																																	
	42																																	
	43																																	
	44																																	
	45																																	
	46																																	
	47																																	
	48																																	
	49																																	
	50																																	
	51																																	
	52																																	
	53																																	
	54																																	
	55																																	
	56																																	
	57																																	
	58																																	
	59																																	
	60																																	
	61																																	
	62																																	
	63																																	
	64																																	
	65																																	
	66																																	
	67																																	
	68																																	
	69																																	
	70																																	
	71																																	

553-5949

Table 1
Trunk Group Access Restrictions worksheet (Part 3 of 4)

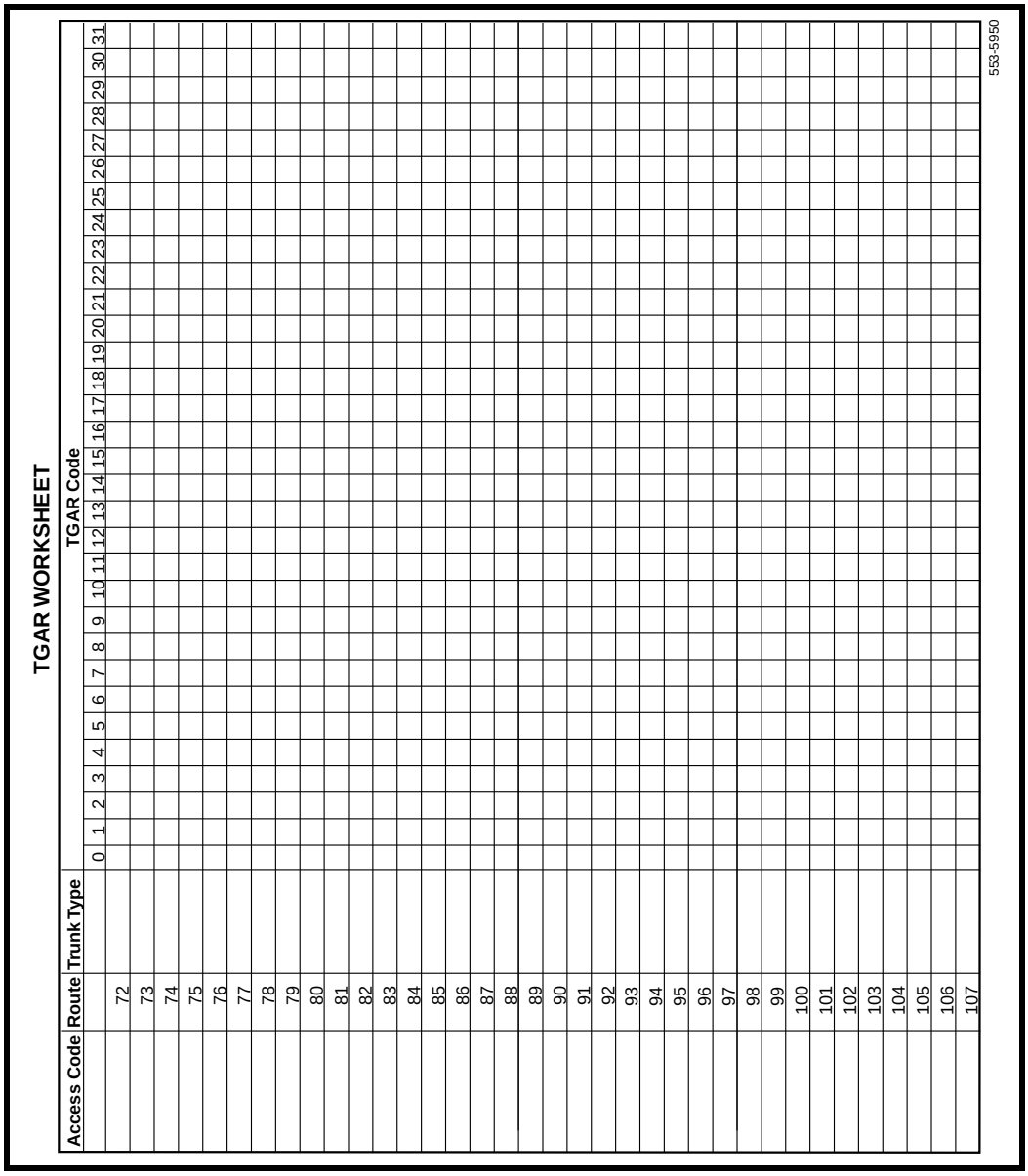
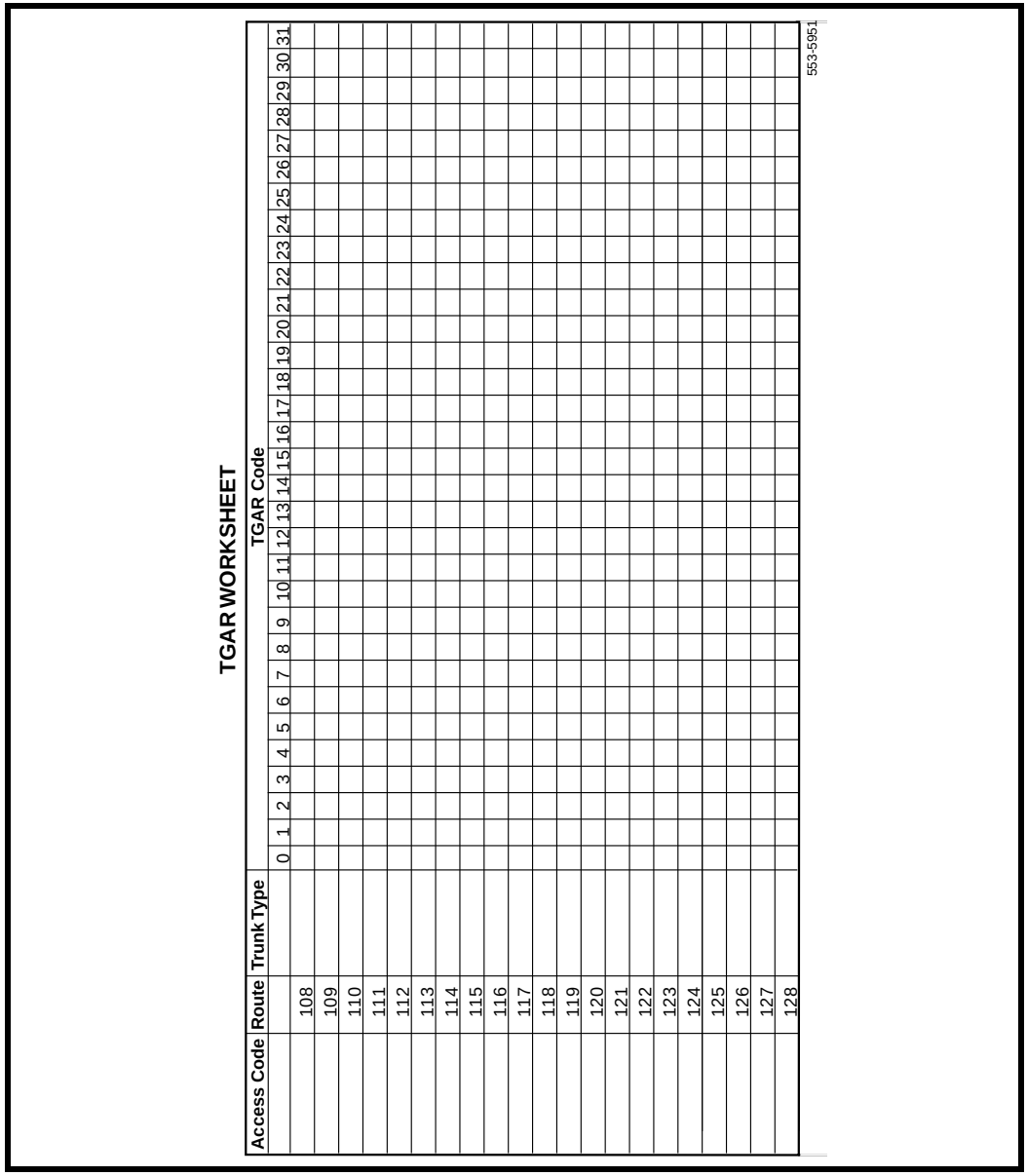


Table 1
Trunk Group Access Restrictions worksheet (Part 4 of 4)



Index

A

A/B boxes, 82
Access Restrictions
    Trunk Barring, 47
access restrictions
    CCOS, 32
    CLS, 20
    CPDC, 36
    CRB, 35
    defining, 19
    ECCS, 33
    ELK, 34
    FCA, 32
    NFCR, 36
    NSC, 27
    SSC, 26
    TGAR, 23
ACD (Automatic Call Distribution), 84
administration program security
    access control, 92
    Audit Trail reviews, 93
    History File, 94
    multi-user log-in, 91
    passwords, 88
    STA, 90
    verifying, 171
administration terminal security, 82
    hardware based restrictions, 82
    switchroom access, 83
AdminPlus terminals, 82
AMIS (Audio Messaging Interchange Specification) networking protocol, 85
ANI (Automatic Number Identification), 20
Application Processor security, 103
    audit checklists, 163
    verifying, 172
ATB (All Trunks Busy) reports, 185, 187
attendant consoles security
    CPG, 73
    ECCS, 33
attendant-extended calls and Trunk Barring, 47
audit checklists
    Application Processors, 163
    Meridian Mail, 157
Audit Trails
    checklist, 130
    LAPW, 92
    reviews, 93
AUTD (Authcode Denied) level, 29
Authcodes
    alarm feature, 29
    checklist, 112, 130
    CLS, 20
    DISA, 169
    Level 1 passwords, 88
    NAUT, 64
    NCOS, 63
    RTCL, 66
    TGAR, 23
    verifying, 169
Authorization Code Conditionally Last, 64, 170
    checklist, 118
    verifying, 170

Automated Attendant feature
restrictions, 79
verifying, 174
AUTR (Authcode Restricted) level, 29
AUTU (Authcode Unrestricted) level, 29

B

Background Terminal
CCOS, 32
checklist, 131
BARS/NARS security, 61
Authcodes, 28
checklist, 117
FCAS, 68
FRL, 63
ICF, 58
ITGE, 67
NAUT, 64
NCOS, 63
SAR, 39
SDRR, 62
SSC, 26
TGAR, 23
TOD, 65
traffic measurement reports, 193
verifying, 169
BUG messages, 94, 195
Busy Hunt feature, 57

C

cable plant records, 97
Call Answering
checklists, 123, 157
Thru-dial, 78
call forward access restrictions, 56
CFO, 60
CFTA, 59
CFW, 59
CFXD, 57
ICF, 58
RCFW, 61
USCR, 57
verifying, 167
Call Forward No Answer feature, 57
Call Sender feature, 79
Call Transfer
Trunk Barring, 47
calling patterns, 14
CAMA (Central Automatic Message Accounting), 36
CCOS (Controlled Class of Service), 32
checklist, 113, 135
ELK, 34
SAR, 40
ccrusr user IDs, 104, 164
CCSA (Controlled Class of Service Allowed)
CPDC, 36
Fully Restricted Service, 21
TGAR, 23
CDP (Coordinated Dialing Plan), 135
SAR, 39
CDR (Call Detail Recording)
Authcodes, 30
checklists, 122, 131, 153
FCA, 32
reports, 178
SAR, 39
CFF (Forwarded Class of Service), 116, 132
CFO (Call Forward Originating), 60, 116, 132
CFTA (Call Forward to Trunk Access Code), 59
checklist, 116, 132
ICF, 58
verifying, 168
CFW (Call Forward All Calls) feature, 56, 59
CFTA, 59
checklist, 114, 115
CFXA/D (Call Forward External)
checklist, 115
verifying, 167
CFXD (Call Forward External Deny), 57, 58
checklists, audit
Application Processors, 163
Meridian Mail, 157

checklists, installation, 109
Meridian 1, 110
Meridian Mail, 123
checklists, security verification, 166
CLS (Class of Service)
assignments, 21
Authcodes, 71
CCOS, 32
CFF, 60
checklist, 110
defining, 20
FCA, 32
implementing, 22
TGAR, 23
CO (central office) security
CPDC, 36
CRB, 35
CTD, 20
configuration analysis, 107
configuration programs and prompts. *See* implementation
COS (Class of Service)
SAR, 37
COT trunks, 62
CPDC (Called Party Disconnect Control), 36, 114
CPG (Console Presentation Group), 73, 122, 134
CRB (Code Restriction), 35
checklist, 113, 133
TLD, 20
CSC (customer service change) activities, 94, 195
CTD (Conditionally Toll-Denied) CLS, 20, 21
CUN (Conditionally Unrestricted) CLS, 20, 21
Customer Night Numbers, 136

D

defining access restrictions, 19
deleting Authcodes, 29
Delivery to Non-users feature, 83, 197
DGT (Digit Manipulation Index), 136
DID (Direct Inward Dial) trunk security
CFF, 60
CFTA, 59
CPDC, 36
CTD, 20
SDRR, 62
digital telephones, 32
Direct Trunk Access and Trunk Barring, 48
DISA (Direct Inward System Access) security, 13, 69
Authcodes, 28
checklists, 121, 137
CLS, 20
ICF, 58
Level 1 passwords, 88
NCOS, 63
NSC, 27
SCOD, 70
service restrictions, 71
TGAR, 23
verifying, 168
X11 release 15 and later features, 201
disabled mailboxes, 80
disabled ports, 96
disttech user IDs, 104, 163
DN (Directory Number) tables, 160

E

ECCS (Enhanced Controlled Class of Service), 33, 113
ELK (Electronic Lock), 34, 113
Enhanced Night Service and Trunk Barring, 48
ESN Data Block, 137
Express Messaging, 78
checklists, 123, 157, 160
verifying, 173
External Call Forward No Answer feature, 57
External Call Sender feature, 79
External Hunt feature, 57

F

FCA (Forced Charge Account), 32
    checklist, 112, 139
    TLD, 20
FCAS (Free Calling Area Screening), 68, 120
FCI numbers, 68
FFC (Flexible Feature Code)
    checklist, 138
    USCR, 57
FR1 Fully Restricted Service, 21
FR2 Fully Restricted Service, 21
FRE Fully Restricted Service, 21
FRL (Facility Restriction Level), 63, 117
    NFCR, 36
    verifying, 170
Fully Restricted Service, 20, 21
FX (Foreign Exchange)
    access, 20
    CPDC, 36
    CRB, 35

G

general security practices, 15

H

History File, 94
    checklist, 140
    multi-user log-ins, 91
    tracking, 195
    traffic reports, 177

I

ICF (Internal Call Forward), 58, 115
IDF (Intermediate Distribution Frame), 97

implementation
Audit Trails, 94
Authcodes, 31
CCOS, 33
CDR reports, 179
CFF, 60
CFO, 60
CFTA, 60
CFW, 59
CFXD, 58
checklists for, 109
CLS, 22
CPDC, 37
CPG, 73
CRB, 35
DISA, 69
ECCS, 34
ELK, 35
FCA, 32
FCAS, 69
FRL, 36, 63
History File, 95, 196
ICF, 58
ITGE, 67
Level 1 passwords, 88
Level 2 passwords, 89
Limited Access to Overlays feature, 93
multi-user log-ins, 92
NAUT, 65
NCOS, 63
NCOS traffic reports, 193
network traffic reports, 183
NSC, 28
Percent All Trunks Busy traffic reports, 188
RACC, 72
RCFW, 61
routing measurements reports, 191
RTCL, 66
SCOD, 70
SDRR, 62
SSC, 27
STA, 91
TACC, 72
TFS40X reports, 189
TFS41X reports, 190
TGAR, 24
TOD, 66
traffic measurement reports, 183
trunk traffic reports, 185
USCR, 57
installation checklists, 109
Meridian 1, 109
Intercept Treatment and Trunk Barring, 48
internal security
X11 release 15 and later features, 201
invalid log-on attempts, 80
ITGE (Incoming Trunk Group Exclusion), 67
checklists, 119, 140
verifying, 171

L

LAPW (Limited Access Password), 89, 92
LD 10 program, 29, 45
LD 11 program, 29, 45
LD 12 program, 45
LD 16 program, 45
LD 17 program, 171
LD 57 program, 45
LD 88 program, 29
LD 93 program, 46
Least Cost Route List traffic reports, 190
Level 1 passwords
administration programs, 88
verifying, 171
Level 2 passwords
administration programs, 89
verifying, 171
Limited Access to Overlays feature, 89, 92
lineman test terminals, 96
LOC (Location Code), 141
Log Files
multi-user log-in, 91
Traffic, 95
log-on attempts, invalid, 80
long-duration call reporting, 189
looping technique, 67

M

M3000 terminals, 33

mail. *See* Meridian Mail security features
mailbox security, 76
    Call Answering Thru-dial, 78
    Call Sender, 79
    Express Messaging, 78
    invalid log-on attempts, 80
    Operator Revert, 78
    passwords, 79, 80, 125
    permission/restriction tables, 77
    Secured Messaging, 81
    User Extension Dialing, 78
    verifying, 172
maint user IDs, 104, 164
MDF (Main Distribution Frame), 96
menu restrictions, verifying, 172
Meridian 1 security features
    BARS/NARS restrictions, 61
    call forward access restrictions, 56
    CDR reports, 178
    checklists, 110
    defining access restrictions, 19
    DISA restrictions, 69
    History File, 195
    modifying access restrictions, 25
    Operational Measurement reports, 196
    security analysis, 175
    security verification, 165
    system reports summaries, 176
    TENS restrictions, 71
    traffic measurement reports, 182
Meridian 1 system access security, 95
    administration program access, 87
    Application Processors, 103
    network facilities, 96
    switchroom, 96
    system administration port, 95
Meridian Mail security features
    administration terminal, 82
    AMIS network protocol, 85
    checklists, 123, 157
    mailbox, 76, 79
    outcalling, 83
    upgrade control, 84
    virtual agents, 84
    Voice Menu/Thru-dialer, 79
Meridian Mail software release 7 and later
    permission/restriction tables, 77
Meridian Mail software release 8
    Express Messaging Thru-dial, 160
    permission/restriction tables, 77
    Voice Menu/Thru-dial, 162
Message Delivery to Non-users feature, 83, 197
mlusr user IDs, 104, 164
modem restrictions, 36
Modify User screen, 78
MTC (maintenance messages), 94, 195
multi-line telephones, 142
Multiple Administration Terminal feature, 82
Multi-Tenants, 71, 121
    SAR, 40

N

NARS. *See* BARS/NARS security
NAUT (Authorization Code Conditionally Last), 64
    checklist, 118
    verifying, 170
NCOS (Network Class of Service), 20, 63
    Authcodes, 28, 71
    checklist, 117
    DISA, 70
    FCA, 32
    NFCR, 36
    RTCL, 66
    SAR, 37
    SSC, 26
    traffic measurement reports, 193
    verifying, 170

network security, 96
traffic reports, 183
X11 release 15 and later features, 201
new system security
Meridian 1 checklist, 110
Meridian Mail checklist, 123
system configuration analysis, 107
verifying, 167
NFCR (New Flexible Code Restriction), 36
checklist, 114, 144
TLD, 20
NPA (Numbering Plan Area) codes
checklist, 145
FCAS, 68
NSC (Network Speed Call), 27, 112, 144
NTCL (Network Control), 143
NXX (Central Office Translation)
checklist, 133
FCAS, 68

O

ODAS (Office Data Administration System), 40
Operational Measurement reports
outcall monitoring, 197
Thru-dial activities, 196
Operator Revert feature, 78, 174
OTC (Originating Trunk Connection), 48
Outcalling
checklist, 157
Operational Measurement reports, 197
restrictions, 83
verifying, 174
Outcalling Detail report, 197
overflow traffic reports, 185
overlays. *See* administration program security
overview, 13

P

parameter values, checklists, 110
passwords
administration programs, 88, 171
administration terminal, 82
Application Processors, 103
changing, 80
checklists, 125, 146, 151, 161
length, 151
mail, 161
mailbox, 79, 80, 125
parameters, 125, 161
port, 96
RCFW, 61
SPWD, 148
STA, 90
USCR, 57
verifying, 171
patterns, fraud, 14
Percent All Trunks Busy traffic reports, 187
permission/restriction tables, 77, 79
port security, 95, 122
Print Only program restrictions, 92
print programs and prompts. *See* implementation
PRT ports, 96

R

RACC (Tenant-to-route access), 72, 121, 152
RCFW (Remote Call Forward) feature, 56, 61, 116
Remote Notification feature, 83, 197
remote system administration, 14, 82
remote telephones, 61
reports, 176
CDR, 178
Operational Measurement, 196
traffic measurement, 182
restriction tables, 123
restrictions. *See* access restrictions
RLI (Route List Index), 147
root user IDs, 104, 163
Route Lists traffic reports, 190
routes, TGAR tables, 205
routing measurements traffic reports, 190

RTCL (Routing Control)
checklist, 119
DISA, 70
verifying, 171

S

SAR (Scheduled Access Restrictions), 37
BARS, 39
CCOS, 40
CDP, 39
CDR, 39
COS, 37
Multi-Tenant Service, 40
NARS, 39
NCOS, 37
ODAS, 40
Speed Call and Network Speed, 40
TGAR, 37
SCH (service change) activities, 94, 195
SCOD (Security Code), 70
Authcodes, 71
verifying, 168
SCPL (Station Control Password Length), 34
SCPW (Station Control Password), 34, 113
SDI ports, 122
SDRR (Supplemental Digit Recognition/Restriction), 62
checklist, 117
verifying, 169
Secured Messaging, 81
security analysis
CDR reports, 178
History File, 195
Meridian 1, 175
Operational Measurement reports, 196
system reports summaries, 176
traffic measurement reports, 182
security verification. *See* verifying
SEER (System Event and Error Report), 82
single-line telephones, 149
SL-1 telephones, 32
Speed Call and Network Speed Call, 40
SPN (Special Number Translation), 150
SPRE (Special Prefix Code), 57, 71
SPWD (Secure Data Password), 148
SRE (Semi-Restricted Service) CLS, 20, 21
SSC (System Speed Call), 26, 111, 151
SSU (System Speed Call User), 26
STA (Single Terminal Access) feature, 90
Station Control Password, 57
Station Specific Authcodes, 29
switchroom security, 83, 96
system access security, 95
administration program access, 87
X11 release 15 and later features, 201
system administration port security, 95
system configuration analysis, 107
system reports summaries, 176
CDR, 178
traffic measurement, 182

T

TACC (Tenant-to-tenant access), 72, 121, 152
TARG (Trunk Access Restriction Group), 23, 111
telephones
checklist, 142, 149
digital, 32
passwords, 151
TENS (Multi-tenant services) restrictions, 71
checklist, 121
CPG, 73
RACC, 72
TACC, 72
TFC (Traffic Reporting), 123
TFC001 traffic measurement reports, 183
TFC002 traffic measurement reports, 185
TFC104 traffic measurement reports, 187
TFN001 traffic measurement reports, 190
TFN002 traffic measurement reports, 193
TFS40X traffic measurement reports, 189
TFS41X traffic measurement reports, 189
TGAR (Trunk Group Access Restrictions), 23
Authcodes, 71
checklist, 111, 120
CTD, 20
NCOS, 63
SAR, 37
tables, 205

Thru-dial security
Call Answering, 78
checklists, 123, 124, 157, 160, 162
Operational Measurement reports, 196
permission/restriction tables, 77
verifying, 172
Voice Menu/Thru-dialer, 79, 173
TIE trunk security
Authcodes, 28
CLS, 20
CPDC, 36
CRB, 35
Fully Restricted Service, 21
ITGE, 67
NCOS, 63
NFCR, 36
SRE, 20
TGAR, 23
time stamps, 92, 93
TLD (Toll-Denied Service) CLS, 20, 21
TN (Terminal Number), 189
TOD (Time-of-Day Routing), 65, 170
TODS (Time of Day Schedule), 119
Toll Operator Break In
Trunk Barring, 48
tracing calls, 36
Traffic Log files, 95
traffic measurement reports, 182
History File, 177
TFC001, 183
TFC002, 185
TFC104, 187
TFN001, 190
TFN002, 193
TFS40X, 189
TFS41X, 189
Traffic Period Option, 185
Traffic Terminal, 153
TRF (traffic outputs), 195
Trunk Access Codes, 59
Trunk Barring, 46
Access Restrictions, 47
Attendant-extended calls, 47
Call Forwarding, 47
Call Transfer, 47
Conference Calls, 47
Direct Trunk Access, 48
Enhanced Night Service, 48
Intercept Treatment, 48
OTC, 48
Toll Operator Break In, 48
trunk security
Authcodes, 28
CFTA, 59
checklists, 153, 155
CLS, 20
CPDC, 36
CRB, 35
Fully Restricted Service, 21
ITGE, 67
NCOS, 63
NFCR, 36
RACC, 72
SRE, 20
TGAR, 23
traffic reports, 185
Trunk Seizure Option, 185
TTY ports, 96

U

UNR (Unrestricted Service) CLS, 20, 21
upgrades, Meridian Mail, 84
USCR (User Selectable Call Redirection), 57, 114
User Extension Dialing, 78
user IDs
Application Processors, 103, 163, 172
verifying, 172

V

verifying, 166
    administration program restrictions, 171
    Authcodes, 29
    BARS/NARS restrictions, 169
    Call Forward access restrictions, 167
    DISA restrictions, 168
    Thru-dial restrictions, 173
VHST command, 94
virtual agents, 84, 141
Voice Mail security
    X11 release 15 and later features, 201
Voice Menu/Thru-dialer, 79, 124, 162
Voice Service Summary reports, 196

W

WATS restrictions, 36

X

X11 release 12 and later, CFTA, 132
X11 release 16 and later
    Audit Trails, 130
X11 release 19 and later
    port security, 96
X11 release 20 and later
    SAR (Scheduled Access Restrictions), 37
    Trunk Barring, 46

Meridian 1 and Succession Communication Server for Enterprise 1000

System Security Management

Copyright ©1993 – 2002 Nortel Networks
All Rights Reserved
Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of the Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users will be required to correct the interference at their own expense.
SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.
Publication number: 553-3001-302
Document release: Standard 7.00
Date: January 2002
Printed in Canada

NORTEL NETWORKS™